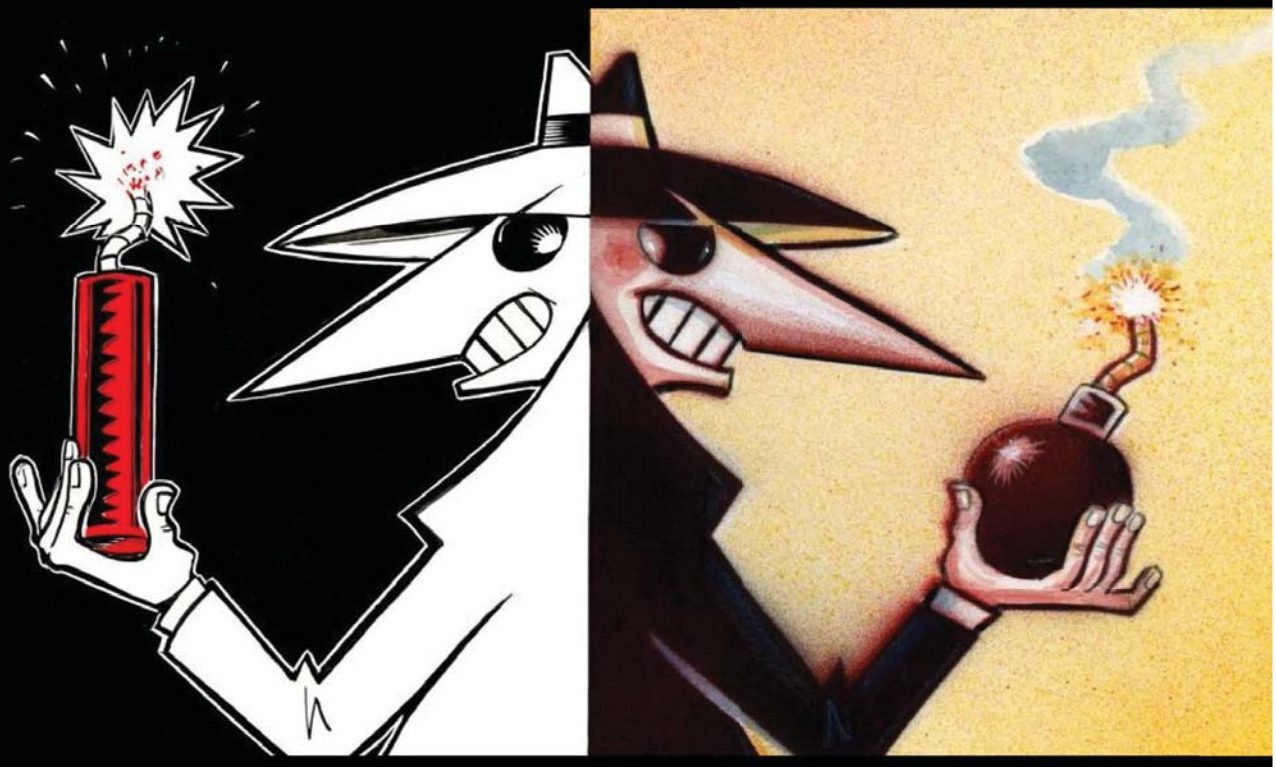
SPY COMMUNICATIONS



SPYCOMM

● CONTENTS

Part I
Background

Introduction 3
Chapter One 7
Modern Examples of Unconventional Communications
Chapter Two 13
Elements of Covert Communications

Part II
Exchanging Information

Chapter Three 23
Establishing Communications Networks
Chapter Four 27
Visual Communications
Chapter Five 45
Bulk Text Message Processing
Chapter Six 53
Guerrilla Cryptography
Chapter Seven 99
Voice Communications
Chapter Eight 121
Disseminating Information

Part III
Technical Aspects of Underground Communications

Chapter Nine 129
Telephone Service Theft and Fraud: A Historical Perspective
Chapter Ten 149
Commercial Circuit Access Strategies
Conclusion 245

I dedicate this book to my father:
"Forty One to Base."

● WARNING

The procedures in this book are *extremely dangerous.* Whenever dealing with electricity, special precautions *must* be followed in accordance with industry standards. Failure to strictly follow such industry standards may result in harm to life and limb. Furthermore, many of the procedures described in this book are *highly illegal* and will result in stiff legal penalties to the offender.

Therefore, the author and the publisher disclaim any liability for any damages or injuries of any type that a reader or user of information contained within this book may encounter from the use of said information. Use this book and any end product or by-product at your own risk. *This book is for information and academic purposes only!*

PART I

BACKGROUND

● INTRODUCTION

Communications is the key element in any covert military or intelligence enterprise. Effective C^3 (command, control, and communications) is what makes things happen at the pace and sequence required for a mission's success. The commander who best employs communications technology will have the most influence on the outcome of the engagement.

Guerrillas, spies, fugitives, and international terrorists all operate in the subterranean world of the "underground." These individuals and groups need to communicate secretly among themselves as well as with supporters and sometimes with the rest of the world. There is seldom any high-tech hardware provided by some third party to conduct these secret exchanges. There also are no actual rules or protocol to transfer the communications safely between the parties involved. Such communications almost always are time-sensitive and critical in nature—missions and lives are often contingent on the communications being sent safely.

Underground operations are conducted for everything from the collection of critical information to the overthrow of a government. Such operations are often faced with an opposition that has more power and better resources. To operate secretly in a potentially hostile

environment requires you to live, organize, and communicate covertly. After all, knowledge is power only when you have the capacity to collect, exchange, and disseminate information.

"Going underground" is more of a constant state of alert rather than an actual place or destination. It means living and operating out of sight. It means organizing and keeping secrets, which must be collected and exchanged like currency or a perishable commodity. It also means taking extraordinary precautions against getting caught.

There is very little enticement or reward for those who choose to operate in this manner. Getting caught conducting covert activities sometimes means getting killed. Very few operatives have the stomach for protracted operations in a high-threat environment, where nothing is as it appears and few participants are worthy of complete trust.

A small cellular team can operate in this environment only with discipline, specific well-defined goals, structured command, and flawless communications. There are no rules in this level of conflict, and there is minimal margin for error. It's a new kind of warfare, and covert communications is the key to success.

This is SPYCOMM, the technology and techniques of collecting and exchanging information secretly. This book will provide a variety of technical communications capabilities for a compartmentalized underground organization. Reliable, anonymous communications using indigenous resources and the existing international communications infrastructure are emphasized, and primitive-to-advanced techniques for exploiting existing facilities already "on the ground" are stressed. This approach is intended to comply with the well-established doctrine of unconventional warfare that places emphasis on improvisational application of existing and alternative technologies as an integral component of covert operations.

Tactical communications can be defined as those

things that you need to learn about your opposition as well as all information about your mission that you need to collect and exchange among elements of your group. Tactical communications in a hostile area between units involved in underground activities requires speed, reliability, and security. Modern "off the shelf" technology can make this happen in virtually any environment if the personnel and equipment are available. Fortunately, most of this technology is already in place in all industrialized and many developing nations worldwide.

Covert communications can be employed as an extremely effective tool in the conduct of an underground enterprise. In fact, it can actually function as a weapon against your opposition. The ability to transfer information secretly among your group or to disseminate it to the target audience involved in a conflict or political struggle can be an incredible asset in any covert operation.

Your ability to communicate covertly may be contingent on your ability to communicate anonymously among the clutter of "legitimate" communications. Being able to improvise a communications network from scratch using only those materials commonly available and being able to conduct communications without a trace are perhaps the most powerful capabilities any operative or team leader can contribute to the conduct of an underground operation.

It should be clearly emphasized to the reader that many of the techniques outlined in this book are focused on the tampering and modification of equipment and services that are owned by the government and/or commercial enterprises. This approach sometimes involves theft or interruption of service. Because of the potential for abuse, this book is presented for information and academic purposes only.

1 ● MODERN EXAMPLES OF UNCONVENTIONAL COMMUNICATIONS

Every day, people around the world use imagination and improvisation to communicate in an unconventional manner while conducting intelligence operations or waging war. Let's look at some recent examples.

GRENADA

During the U.S. invasion of the tiny Caribbean island of Grenada in 1983, the accelerated characteristics of fire and maneuver during the large-scale assault created some periodic, temporary losses in small-unit C^3. In one widely reported incident, a small U.S. Marine reconnaissance unit found itself pinned down in an unoccupied building during a firefight with Cuban military advisors. When the squad's forward air controller (FAC) attempted to reach rear echelon command to request a fire mission, the radio link failed.

Instead of panicking or attempting a withdrawal from the area, the unit's commander found a working telephone inside the building. He contacted the overseas operator and asked to be connected with the Pentagon in Washington, D.C. The operator refused to place the call because of a lack of billing information. One of the marines gave the operator his parent's long-distance tele-

phone credit card number and the call was put through. The marine explained the situation to one of the duty officers at the Pentagon and requested air support.

Within minutes the fire mission request was relayed to the Marine Corps command on the ground in Grenada and approved. The ground trembled outside the building protecting the stranded reconnaissance unit as rocket fire was brought down on the enemy positions. Quick thinking and an improvisational mind-set enabled this elite small unit to communicate and carry on.

AFGHANISTAN

During the war in Afghanistan, a psychological warfare operation was developed by Central Intelligence Agency (CIA). A small FM radio transmitter, no larger than a pack of cigarettes, was connected to an auto-reverse Sony Walkman cassette player. The tape was a message in Russian offering Soviet troops a variety of incentives for desertion. The transmitter broadcasted the message continuously on Russian tank radio frequencies, where lonely Soviet conscripts spent hours in the hot, cramped crew compartment monitoring the radio.

The boredom and searing heat probably contributed to the impressive success of this classified operation. Many Soviet soldiers showed up at the Pakistan border willing to surrender weapons, ordnance, and, in many cases, vehicles and documents in exchange for the terms presented by the miniature "pirate" radio stations.

MOZAMBIQUE

In 1987, guerrillas operating with RENAMO in Mozambique were provided anonymous assistance with covert communications in their fight with the socialist regime. In the dense jungle of one of the poorest countries on the African continent, semiliterate native guerrillas

used Tandy Model 100 lap-top computers interfaced with solar-powered FM transceivers to maintain high-speed digital communications links with command elements. This low-cost, sophisticated, off-the-shelf technology is fairly secure when properly employed.

BELIZE

In a remote section of jungle in the Central American country of Belize, a young man has built and installed his own television system. He has hooked up a satellite dish to pick up American commercial broadcast feeds directly off of the orbiting communications satellite. He decodes these signals and then broadcasts them over normal TV channels. Local villagers are provided with televisions operated by car batteries and charged a couple of dollars a month for this homemade subscription television service. He has complete control over all local programming, and if enough people are late with their monthly service fee, he simply shuts the entire "network" down until the villagers take up a collection and settle their accounts.

In an uncharacteristically stable and friendly country bordered by several contested regions in Central America, a segment of the local population is exposed to U.S. media and commercial marketing. This is a unique, creative approach to exposing the American way of life to a small, impoverished nation without foreign aid or significant U.S. government involvement. Although somewhat unconventional, this particular case is generally considered to be conducive to positive relations with the United States and is peripherally consistent with U.S. foreign policy objectives in the region.

PANAMA

In 1988, the brutal regime of Panamanian dictator Manuel Noriega had complete control over all broadcast-

ing and print media. A small group of Panamanian exiles and dissidents living in the United States created several "underground" newspapers using home computers and desktop publishing software. These publications were sent by fax machine to various anti-Noriega elements in Panama, who printed camera-ready newspapers on ordinary copy machines and distributed them throughout most of the major urban centers in the country.

Although Noriega appeared almost every night in front of adoring crowds on his state-run television news programs, these covert underground newspapers were fostering and developing growing discontent. In fact, in the aftermath of the December 1989 U.S. invasion of Panama, independent polls indicated that 83 percent of Panamanians supported the overthrow of Noriega.

U.S. foreign policy objectives were met with the support of friendly indigenous personnel, careful orchestration of the demise of Noriega's public image in Panama, and, ultimately, with minimum military force.

ROMANIA

Unlike Panama, the government of Romania was a well-entrenched, tightly controlled, and constantly guarded dictatorship. All media devices—including typewriters, photocopy machines, printing presses, broadcast and print media, school books and curriculum, and music and entertainment—were strictly censored by the state and tailored to reflect the regime's objectives and policies.

Outside influences still had a significant impact on the population, however. Voice of America, Radio Free Europe, and various commercial and government shortwave radio broadcasts did reach individuals in the tightly controlled population, and the seeds of discontent were carefully planted over several decades. As the reform movements and democratic develop-

ment of neighboring East European nations became common knowledge in Romania, dissident groups became more openly vocal about their discontent. When the regime of dictator-for-life Nicolae Ceausescu attempted to impose the textbook communist response of violent reprisals against dissidents, this too was reported, and the response from the population was immediate and violent.

What is notable about the popular uprising in Romania is not just the rapid pace of developments but also the tactics employed by the supporters of the coup. Instead of protracted guerrilla warfare or acts of terrorism to attack the government's infrastructure, they simply had to seize one minor piece of real estate to win the confrontation—the state-run television and radio center in Bucharest. The dissidents seized the media center and with it the attention and support of the population. Once they gained access to the masses, all that was left was to execute the leadership.

The public execution of the Ceausecus was seen on every TV screen in Romania and throughout the world, graphically demonstrating the power of communications. The dictatorship created a centralized media system that ultimately communicated live and in graphic terms the demise of the dictator and his wife in front of a firing squad. This, of course, did not solve all of the problems or instantly create a stable society in Romania, but the point is that the world watched a small voice of dissent grow into a roar of popular uprising with the seizure of communications and access to the masses.

• • • • •

Every day around the world, small groups of people are using communications technology to operate covertly in hostile settings to reach large numbers of people with an alternative message, and to influence the way these

people perceive themselves and their society. Indeed, communications technology has been and is being employed to inform the masses, influence opinions, conduct wars of liberation, overthrow governments, and change history.

Going underground to conduct a covert operation has become much more viable because of improvements in communications technology. An underground organization can employ a number of alternative electronic technologies to greatly enhance the effect of the enterprise. Communications can be seized, borrowed, or bootlegged to gain access to other members and even to create a large organization in a short period of time.

Underground communications technology can allow the clever and persistent organization to have a great deal of impact on a society or an audience. This nonviolent approach can be devastating to the opposition. As seen in the above examples, governments have been influenced and sometimes even toppled with minimal violence because communications were used as the tool of the dissident.

Whether you need to communicate with a small group of individuals in an underground organization or require a means of accessing the masses, communications technology can be the most effective tool available. The operative must use imagination and creative tactics to exploit the existing infrastructure and get the message sent to the right person or audience cheaply and without getting caught. Yet the act of communicating covertly is one of the risky elements of the conduct of the operation it supports. A clear head and careful planning are essential to the safe, effective use of underground communications.

2 ● ELEMENTS OF COVERT COMMUNICATIONS

Communications is both an art and a science. It can be defined as the practical art of expressing thought, instructions, or ideas. It is also the science of managing and transmitting information.

Covert operations is a more abstract term. Covert is generally construed to mean disguised or concealed. A covert operation may be an active or passive enterprise, usually focused on specific individuals or groups of individuals. It must conceal its existence, intentions, and techniques during planning and execution. (In fact a true covert op is *kept* secret even after the mission is completed.)

Covert communications is the science of exchanging information without detection, disseminating information without permission, and collecting information without the knowledge or consent of the target. Covert communications is also the art of concealing the transfer of information.

Various aspects of underground operations must be considered before a reliable method of secure communications can be created and implemented. In military or intelligence operations, these aspects are known as the *Essential Elements of Information* (EEI).

ESSENTIAL ELEMENTS OF INFORMATION

Military intelligence is intended to collect, process, and disseminate EEI in the conduct of war. In conventional land warfare, specific facts are "mission essential" to the conduct of the operation. These facts typically are based on terrain, weather, and the enemy. The commander who has the most timely and accurate information regarding these three areas generally can exert the most influence on the outcome of the engagement.

For example, an understanding of the tactical aspects of the terrain allows the most effective use of available cover, seizure of the high ground, or interruption of the enemy's lines of communications. Being prepared for the weather and exploiting its conditions can be deadly offensive tools in small-unit actions. Hard intelligence on the intentions, capabilities, strengths, and weaknesses of the enemy allows the commander to destroy him with less effort and in less time.

In covert operations or unconventional warfare, these elements are also applicable to some degree. There is, however, always much more information required than these three specific areas. The fundamental difference is that although you are faced with an opposing force (OPFOR), you seldom have the intention of or capability for direct confrontation. Rather, you often are conducting your mission among elements of the OPFOR on terrain occupied by the OPFOR. Unless you understand EEI, your survivability under these conditions is historically quite poor.

Operating Covertly in a Hostile Environment

Anytime you wish to conceal information about yourself or your activities, you are involved in a covert operation. Furthermore, whether you are participating in an undercover narcotics investigation, gathering corporate intelligence for a competing firm, or for one reason or

another forced to go underground, you are operating in a hostile and potentially dangerous environment. Your *immediate* threat is not capture or confrontation—it is operational compromise.

In order to operate securely in a hostile environment, EEI for any covert operation must be outlined completely to all participants. They will include, but will not be limited to, the following:

1. TERRAIN. Detailed maps and knowledgeable "guides" are vital to understanding the area, establishing penetration and extraction routes and alternates, and knowing where unforeseeable or random events might occur on a regular basis. The locations of safehouses, drop points, meeting and contact areas, and local opposition strongpoints are all factors of terrain. The "terrain" may be a building, city, or country.

2. POPULATION. An understanding of the indigenous population is essential for operational existence among them. Ethnic, religious, occupational, and recreational information is of particular use. Whether you intend to penetrate a "clique" of people, factory, small community, or major urban area in a foreign country, your understanding of the general characteristics of the population, regardless of its size, is essential.

3. HISTORY. Background information regarding individuals, areas, groups, or conditions in the target area is most useful. The facts regarding the criminal history of an individual you may have to recruit or study, the ancient history of why one group will always hate another group in the target area, and the constantly changing political and economic history of an area or group of people are all useful bits of background that can be exploited as you try to accomplish your secret agenda.

4. OPPOSITION. The opposition will, of course, include enemy forces who will actively search you out. But more importantly, the opposition is also comprised of peripheral individuals and groups who might frown

on your activities. The means by which spies, unconventional warfare operatives, and even criminals and terrorist groups are defeated is often related to information provided to the active opposition by passive elements within the local population. It is vital to understand that informants can be more of a direct threat to you than the actual enemy.

5. RESOURCES. Resources are often what make a covert operation happen. Outside support for the insurgency is considered the most vital factor in a protracted guerrilla war.

Resources from within are also a significant factor. Identifying and then exploiting available materials and personnel is what makes virtually any covert operation a success. Your ability to exploit these available resources, both openly and covertly, is based upon your individual skill and knowledge of how to best do so.

Resources are not just tangible materials or personal participants in a covert operation. Resources can also be *conditions* that can be exploited. The accurate depiction of the corruption and conditions caused by a tyrannical dictatorship is a significant resource that can be harnessed to create and maintain an indigenous population's "will to fight."

• • • • •

Understanding the basic concept of EEI is critical before the operative attempts to develop a means of covert communications for a specific operation. Failure to completely understand one or more of these five areas has compromised more operations, caught more bad guys, and killed more agents than all other factors combined. The means by which you maintain contact among active personnel as well as with any "target audience" must be carefully tailored to the terrain, population, history, opposition, and resources available. Understanding

this obvious prerequisite, let's examine the critical areas of covert C^3.

COMMAND, CONTROL, AND COMMUNICATIONS (C^3)

The essential elements in any underground communications network are:

1. SECURITY. Covert message traffic must be designed to protect the content of the message. Equally as important, the means by which the message is exchanged must be designed to protect the sender and the receiver. Above all, the measures taken to protect content and participants must not, by their very nature, call attention to themselves while meeting the basic security requirements. In other words, if the opposition can determine that you are sending covert communications, you are in as much danger as if they understood the content of the message in the first place.

This concept cannot be stressed enough. Operational compromise occurs more frequently in covert work due to detection or capture of agents in the process of sending obviously encrypted traffic than it does from any other aspect of communications. Paraphernalia and devices designed to provide communications security (COMSEC) should never be employed in a manner where their very presence causes compromise. Avoid those technologies that provide some degree of COMSEC but require elaborate physical security.

2. RELIABILITY. Underground communications must be designed to function without failure under exceedingly unpredictable conditions. Any system or device that requires constant maintenance by skilled technicians or substantial operating skill to deploy effectively under adverse conditions is essentially worthless. Networks that require constant monitoring by human operators or that are for one reason or another "time-intensive" to

employ are of no value. Reliability means having constant backup and contingencies planned and practiced by all elements. Reliability means simplicity—nothing hard to perform or complicated to remember.

3. FLEXIBILITY. Regardless of how secure and reliable the communications system, there is always a substantial possibility that the security measures will be defeated or penetrated or the system will temporarily fail or break down. Therefore, one must maintain a flexible mind-set. Flexibility is easy to define but often difficult to teach or instill in even the most clever operative.

Flexibility is not simply a specification of hardware capabilities; it is also a state of mind. Imagination combined with a well-developed "improvisational mind-set" should be a prerequisite to admission to an underground cell. It eliminates dependence on a prearranged plan and allows the operative to employ whatever resources he can access to securely communicate even if the intended materials are not available. Such a mind-set eliminates panic in an urgent or dangerous situation where communications are vital.

4. SPEED. In underground communications, there is clearly a "need for speed." Covert communications must be transcribed into a "normal sounding" code rather quickly, and it must be decoded just as fast. The actual transfer of the message from sender to user must also be rapid. This makes for more secure traffic and decreases the likelihood of compromise. The faster the transaction, the less reliance on whatever method or hardware involved; thus more reliability is achieved.

The focus on speed is also beneficial to message format. Codes for both priority and routine traffic must be implemented to reduce on-air or connect time. This promotes rapid understanding and the ability to interact and respond in less time. Thus, command and control decisions can be made faster. Additionally, well-executed fast transactions tend to be better organized and less cluttered

with worthless or nonessential information. Since transmissions must be carefully thought out before being sent, they are likely to contain accurate, timely information.

5. ACCESS. In general, a communications system must employ existing facilities already "on the ground" in the target area. Access to these facilities must appear to be quite ordinary. This approach is generally safer, more reliable, less expensive (your operation likely has a limited budget), and faster than installing your own system. There are many techniques using existing technology and hardware to which you and your operatives have access that will provide a higher degree of security and a smoother transfer of essential information than your own deployment of specialized hardware to accomplish the same thing.

• • • • •

Regardless of whether you are collecting, exchanging, or disseminating information, the above five criteria must be considered in your operational planning. If, for example, you are attempting to maintain contact with a worldwide network of paramilitary personnel for message or fund transfers, you must carefully consider all of the above areas. If you want to reach a mass audience illegally, it is important to consider the medium to which the target audience has reliable access. If you are recruiting dissidents or insurgents in a foreign country, flexibility, speed, and security are vital. If you understand the essential elements of your communications system, you will expend less time experimenting and more time using your creative energy to develop methods and technologies that are most suitable for your agenda.

PART II

EXCHANGING INFORMATION

3 ● ESTABLISHING COMMUNICATIONS NETWORKS

The efficient flow of operational details, assignments, logistic requirements, and intelligence information is the most critical aspect of any covert operation. This section focuses on a variety of methods to exchange messages in a manner that is intended to elude detection. These techniques certainly are not foolproof or applicable in all situations, and many are illegal or unethical. One fundamental consideration for the operative is that anytime an illegal tactic is used to communicate sensitive information, the act of sending the information becomes as dangerous as its content. Sound judgment and common sense are critical.

Another critical aspect in underground operations is the clear understanding of chain of command. Your operation will almost always take on a military or paramilitary structure in order to maintain effective control of all elements. The communications, or COMMO, plan must meet the specific needs of all echelons.

Underground groups typically operate in carefully isolated and compartmentalized *cells*. Each cell is actually a mini organization with a personality and structure all its own based on its mission. Cell members only affiliate operationally among themselves, although the identity of each agent often is further isolated from all other

agents in the cell. Cells have no means of establishing contact with other cells, and each has a commander and a second in command who can contact the organization's actual leadership.

The exception to this is the *action cell.* It often is a close-knit and interdependent group of guerrillas who must trust each other with their lives. They must plan, train, and function as a team. Operational tasking for an action element is conducted by the element's commander only. In fact, the actual organization may have no knowledge of the identity of the individuals in the action cell. The cell commander is given a mission to perform, and he is often left with the complete control of selecting, training, and arming his team with specialists from the underground community who would be suitable for the given task.

Other cells may be assigned technical or logistical tasks that establishes their individual characteristics and communications needs. A cell that continuously monitors the opposition's radio traffic, for example, may function in an agent/handler configuration. (A *handler* recruits and supervises, or *runs*, agents by contacting each on a one-to-one basis to meet the specific needs of the individual and to collect intelligence. Generally, he answers directly to the operation commander.) A cell that is assigned the task of maintaining safehouses or meeting places may function in an entirely different way and have much different intelligence and communications needs.

The commander of an underground organization uses a variety of communications mediums to maintain command and control over all these isolated cells in a manner that keeps him and all other participants as separate and controllable as possible. He executes the mission from a concealed and generally mobile *command post* (CP). The CP must maintain contact with all first-echelon cell commanders through a covert command network.

It is up to the *communications officer* to create a com-

prehensive communications plan. The plan must take into account the mission and all EEI to create a number of separate communications networks that have pre-established priority. Though your requirements may include other networks, the following should be included:

1. COMMAND NET. This is the highest priority communications network in the system. Instructions and orders are sent along this network by the overall commander of the operation to individual cell commanders. Operatives are not authorized to use this net, nor do they generally even have access to it.

2. INTELLIGENCE NET. This is the second highest priority network. It also serves as an alternate COMMO net in the event the command net is compromised or destroyed.

This network is designed to provide command with time-sensitive intelligence relating to EEI, situation reports (SITREPS) regarding specific actions, and any immediate requests for support that will affect the outcome of the mission. The intelligence net also covers operations and is often called the INTEL/OPS net.

3. DIRECT ACTION NET. Due to the sensitive nature of the use of force in an underground operation, all "action element" commanders are provided a separate network to coordinate an action as well as to receive activation or abort commands and threat warnings, target acquisition information, and so on. The direct action net is carefully controlled and "cut out" from all other areas of the system. This compartmentalization provides isolation from other aspects of the operation to protect both the participants in the action and other members of the operation.

4. ADMINISTRATION/LOGISTICS NET. The ADMIN/LOG net provides all operatives with basic support needs. Coordination of safehouses, financial support assets, materials, and weapons are "sourced" through this network.

By compartmentalizing communications system into several networks, the following critical conditions are established:

1. ISOLATION. By having several communications networks to conduct an operation, you achieve a degree of "damage control" if any one net is compromised. For instance, if the ADMIN/LOG net is compromised, the opposition will have acquired only specific information regarding logistics. Your overall objective is not compromised by the security failure of any one net.

2. FLEXIBILITY. Should any net fail, you are not automatically out of business. Compartmentalization allows you to fall back on preset backup planning. Until the command network is restored, for example, you can employ your intelligence net to communicate.

3. ORGANIZATION. Separate communication networks allow different aspects of an operation to proceed simultaneously. Routine and priority traffic can be established and maintained on each network. Individual command requirements, organizational tasking, and overall information flow will run smoother and with less "clutter."

4 ● VISUAL COMMUNICATIONS

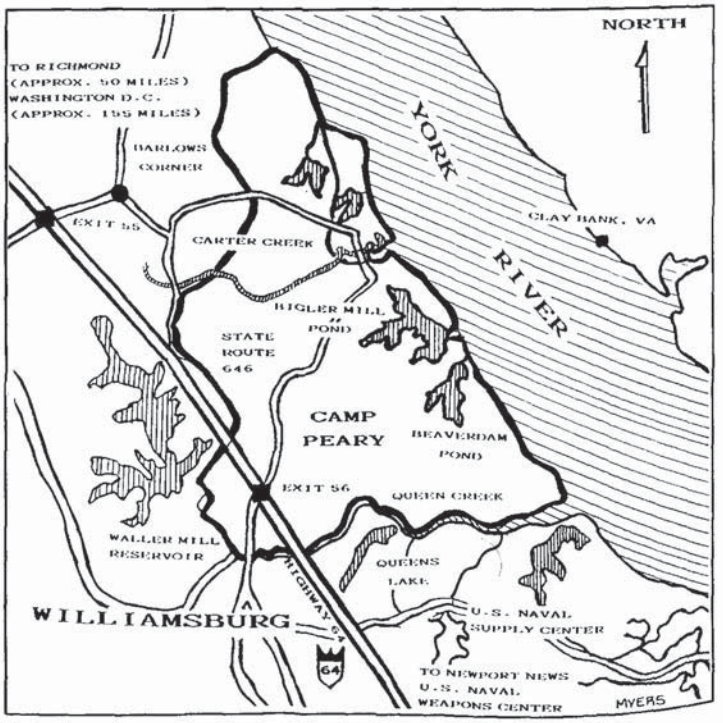
Sending information visually encompasses written messages, covert signalling, and face-to-face meetings. Visual communications can also be conducted by electronic means—including photographic intelligence (PHOTINT), video, facsimile (fax) image, and more sophisticated hardware—though this is not always possible or practical from a security or economic perspective. Therefore, this chapter will focus on the nonelectronic transfer of visual communications.

The clandestine exchange of visual communications is an ancient form of "tradecraft" taught and used by every intelligence or underground enterprise for literally thousands of years. One of the best schools for this activity is operated by the U.S. Central Intelligence Agency.

Candidates for the Clandestine Services of the CIA are sent to a secure government training facility to learn the various aspects of tradecraft. This facility, officially known as Camp Peary, is located just outside Williamsburg, Virginia, about 50 miles from Richmond and about 155 miles south of Washington, D.C. This 10,000-plus-acre wooded facility is on the western slope of the York River and to the east of Interstate Highway 64, between exits 55 and 56. To the north of the camp is the York River State Park, and to the south is the U.S. Naval Supply Center.

Old CIA hands from the 1950s called Camp Peary "Camp Swampy" because large portions of the facility were muddy, inhospitable marshlands full of mosquitoes. More recent graduates call it "the Farm," and it has become the subject of fiction and legend in spy circles.

Camp Peary is guarded by armed U.S. Marines and security personnel. A chain link fence with barbed wire and electronic intrusion devices surrounds the entire facility. It has a private airstrip with a large letter R in white painted on the runway—presumed to indicate that landing rights are restricted.



Camp Peary, Virginia (AKA "the Farm"). Approximate location: 37°, 16' Latitude North; 76°, 36' Longitude West.

Camp Peary served as a Navy Seabee training facility and a POW camp for captured German soldiers during World War II. Because of these past uses, there are several obstacle courses, weapons ranges, and an area that serves as a mock interrogation facility on-site. Two creeks and a number of ponds on the grounds are used in training as well as for recreation, since fish are abundant. The camp has an excellent gym, swimming pools, and other physical training facilities such as jogging trails. Large brick buildings serve as classrooms and quarters for the trainees during the sixteen-week initial training in covert operations.

The official CIA cryptonym for the facility and its training program is ISOLATION. The orgins of this term seem to be based on the fact that certain foreign governments friendly to U.S. interests have arranged to send some of their intelligence people to the Farm for training. These individuals are flown directly from their countries to Camp Peary; many, in fact, have no idea they are even in the United States while being trained by language-qualified CIA personnel.

In less than four months, the trainers at the Farm teach the basic tactics and techniques of covert operations. The trainee is exposed to physically demanding and arduous conditions while learning the realities of clandestine operations, from essential paramilitary skills such as hand-to-hand combat and light weapons handling to lectures on past CIA successes and failures in covert ops.

Trainees are taught that intelligence work is a fluid and constantly changing endeavor. It can be mundane and exciting at the same time. It requires initiative and excellent interpersonal skills, since the future handler must observe, assess, and approach potential agents in a very specific way intended to protect the process until the prospect is "hooked" into the enterprise. Covert communications, devised in a well-thought-out, generally quite clever *COMMO plan*, provides agents with instruc-

tions and assignments, as well as the means by which they are paid and expected to provide specific bits of intelligence *product* to the handler.

The specific techniques of communicating with agents that the future handler will recruit and run are probably the most heavily covered and stressed topic. The COMMO plan is designed to collect and exchange information secretly using these age-old techniques. These essential skills are also taught at other infamous espionage schools such as the Midrasha outside Tel Aviv, where Mossad agents are trained, and the KGB school at Dzerzhinsky Square in Moscow.

No matter where the skills are taught, the danger of compromise is always addressed. Trainees are taught that the clandestine exchange of information is the most dangerous part of running a cell of agents. If any aspect of the operation has been placed under scrutiny by the opposition, it is likely that they are waiting to confirm their suspicions by catching one or more participants in the act of transferring information. Case histories are discussed to establish the hazards of clandestine exchanges and leave little doubt in the trainees' minds of what will occur if they or one of their operatives are detected in the process of covert communications.

EXCHANGE SIGNALS

The most critical part of a COMMO plan is the ability of each participant to be able to signal the need to communicate before the actual exchange of information occurs and indicate the method or medium of the exchange as well as the priority of the message. A situation where the agent simply services a prearranged drop on a regular basis is rare. Covert work is too dynamic for anything so habitual.

The trainee is instructed in the art of signalling—the creative use of prearranged, generally nonverbal, anony-

mous cues that indicate the need by one participant to communicate a visual message to the other. The primary operational characteristics of this approach are to provide both the agent and handler with the ability to conceal their need for communication from the opposition, as well as to determine the priority of the message and the authenticity of the sender. Again, all this should occur *before* the actual exchange.

The meaning of several signals must be established. These include:

1. I HAVE A MESSAGE TO SEND. This is accomplished by alerting the contact with a prearranged signal. It could be the presence or absence of a light or object in a window, the placement of an innocuous advertisement in a local paper, or simply a collect telephone call to a "wrong number" at the contact's residence. The medium employed is *never* associated with the one used to actually send the message.

2. MY MESSAGE IS URGENT/IMMEDIATE/ROUTINE. The priority of the message is included with the sign for the need to communicate. In other words, the message would be understood as, I HAVE AN URGENT MESSAGE TO SEND. The priority of the traffic is important for many reasons. An informant may have time-sensitive intelligence about your target, he may need funds or some sort of help, or he may simply need to find out what he is supposed to be doing with a specific case.

Upon receiving a clandestine signal that a specific priority message exchange is needed, certain information must be conveyed in order to receive the message safely.

3. AUTHENTICITY. Regardless of how cleverly you have arranged to signal that a message needs to be exchanged, it is critical that you also have a prearranged group of signals that indicate that the message is valid and being sent by the right person.

It should be obvious that when you are arranging the transfer of visual information, you or one of your opera-

tives can be compromised. Therefore, as a vital safeguard, a *duress warning signal* must be established. This indicates that while the party attempting to send the message authenticates its validity, he or she is doing so under duress. This person has been compromised and is being coerced into uncovering the operation, and his ability to appear to be cooperating is frequently what keeps him or her alive. You must recognize the duress warning signal and *appear* to be willing to acknowledge the source and authorize the exchange.

If the duress warning signal is present, your agent may die if you ignore him. Yet if you do not ignore him, you will probably be compromised yourself to some degree. Arrange the message transfer only after assessing the potential damage. If your message is designed in a way that it is completely anonymous, it would be impossible for the OPFOR to isolate you specifically as the recipient. Unfortunately, if you have had any contact with the agent under duress and he is trying to contact you with a message, your identity has probably been established by the opposition already.

What is important here is that all parties accept and understand what will happen if the duress warning signal is sent. If you are conducting a dangerous intelligence operation, advise all participants that if they are compromised and the signal of duress is sent, no assistance or cooperation will ever be provided at the expense of the operation. You will, however, use all of your resources to influence the opposition to release your agent.

It is important that each member in a cell at least believe that if he is captured or compromised, you as the commander or handler will go to great lengths to protect him. This cannot be stressed enough. If the operative sending the duress warning signal believes that it will only protect the cell and the operation, he is unlikely to send it. It is left up to you to establish what actions to take in support of the party sending the duress warning signal based

on the operation, the individual participants, and the risks. Again, it is vital for all cell members to believe that sending the duress warning will not only protect the operation but also benefit them in some immediate way.

Upon determining that the message signal is authentic and not sent under duress, you must then confirm receipt and arrange the exchange.

4. CONFIRMATION. This acknowledges to the party wishing to communicate that you understand and accept the signal. It is done by some prearranged indicator, such as a specific number of matches removed from a matchbook and thrown down in a specific location or a certain arrangement of window curtains. The confirmation obviously should be different from the initial signal.

5. ARRANGEMENT TO EXCHANGE. The signal that is sent with the confirmation should also indicate what method you want to use to make the exchange of information. There should be a wide range of prearranged choices. For example, the confirmation signal could be the placement of a specific brand of food on a shelf in a supermarket at a specific time. Casually mixing one brand of product a set number of shelf items from where it belongs could indicate that the message is confirmed and the exchange will take place at dead drop number 3.

CIA trainees are provided with a variety of suggestions for creating a clandestine signal system in any environment. Though it is up to the trainee's imagination to create his or her own methods, there are three important characteristics of any message signal system:

1. The system should be quite "normal" in appearance and not betray its intent, even under close professional observation. It should be integrated as part of the operative's routine.

2. The actual transfer of the signal should be done in an anonymous manner, such as through a publicly accessible medium or along a well-traveled route.

3. The essential elements of the various signals

should be completely separate from each other. The request to send should not be related to authentication. The duress warning signal should not be a specific signal but rather the absence of a specific signal. The confirmation can contain the arranged method of exchange, but the actual method must be predetermined.

The important aspects of exchanging visual information—the request to do so, the verification of the authenticity of the request (and if it is or is not under duress), and the confirmation and arrangement to conduct the exchange—must be carried out so they isolate the OPFOR from knowledge of the contact. Creative use of the environment can permit two parties under professional surveillance to get the message signal across without much risk. Assumption of being observed and carefully scrutinized, acceptance that the transaction may be compromised, and determination to accomplish the exchange in spite of these factors is what gets the signal sent.

A useful hint in creating a covert signal system is that the five elements involved with the transaction should be established on a one-on-one basis with each operative. Although the essential elements should always be stressed, each operative can develop his own approach for individuals in his cell. In most cases, the signals should be focused on the absence of something instead of the presence of something. More sophisticated approaches, such as the slight alteration of an object or image, can be useful; however, simplicity is paramount to reliable signal transfer.

The need to communicate face-to-face is the most dangerous aspect of underground communications, and it is only done because of a specific need to interact with the individual, such as for briefing, debriefing, or recruiting. Although extremely risky, face-to-face meetings are frequently essential. They can provide the commander with the ability to assess nonverbal cues and characteris-

tics that cannot be communicated by radio or telephone or expressed in writing.

As you study your environment and activities to create a message signal system, remember that the various signals are somewhat interchangeable in format. Create your list of possible approaches to signalling, assess the value of each approach, then select a method for each stage of the process.

EXCHANGE MEDIUMS FOR VISUAL COMMUNICATIONS

The "medium" employed to make the exchange is also stressed in training. A medium can be an object, place, or person.

The standardized content of the actual message should be established. The typical rule here is that the message should be as small as possible. If sending photographs, for instance, the message should be in the form of exposed film or microfilm concealed in a small, ordinary object. If the operative needs to exchange written notes or text, the material should be encoded, reduced in size, and concealed in a small package. For example, an 8 1/2 x 11-inch, single-spaced typewritten page can contain about five hundred words of encoded text. This can be physically reduced several times on an ordinary photocopy machine. If the copier is fairly good, the 8 1/2 x 11 sheet can be reduced to the size of an ordinary 2 x 3 1/2 business card. This can then be rolled into the bottom half of a cigarette, which can be lit, partially smoked, and put out in an ashtray in a hotel lobby or before entering an elevator.

CIA trainees are taught a number exchange mediums. Three ancient concepts are the dead drop, live drop, and brush pass.

Dead Drop

A *dead drop* is a physical location that is used for the

unattended exchange of the message. It has significant advantages in several areas:

1. The two parties exchanging information don't have to be present simultaneously to conduct the exchange.

2. Third parties can be employed to make the drop as well as service it.

3. The actual timing of the exchange is usually flexible.

There are also disadvantages to a dead drop. Some that should be carefully considered:

1. The message is left in an area that is accessible to the opposition. If the OPFOR discovers the drop location, they can attempt to intercept both the message and the participants in the exchange.

2. Due to the temporary lack of physical security of the message, it must be encoded. Possession of an encoded message is incriminating and dangerous.

3. Dead drops generally are in accessible areas where different conditions and circumstances can affect the transfer. Random, unforeseeable events may affect the drop.

Overall, a dead drop is an excellent clandestine message medium. The transfer of messages in this way has one significant feature that outweighs all the negative aspects—the content of the message is not affected. If an agent needs to exchange any type of formatted traffic—including written, photographic, audio, or video traffic—the dead drop can be employed. The drop can also be used to transfer logistical support materials such as weapons, ammunition, electronic communications equipment, or collection devices.

There are three basic criteria for a dead drop:

1. It should be in a "neutral" area located along a well-traveled route (e.g., crowded public areas).

2. It should be physically difficult to surveil while maintaining a realistic number of approach and escape routes. Public libraries, rest rooms, and transportation facilities are all suitable.

3. Its physical appearance should not betray its con-

tent. It should be something that can permit placement and retrieval quickly and without appearing to be out of the ordinary.

A dead drop should be seriously considered as an option for clandestine exchanges. Your environment contains literally millions of potential locations that can be utilized—the creativity of the operative is the main ingredient in determining which will work for the specific situation. The following locations and methods have proven to be quite useful as dead drops in urban areas.

1. PUBLIC TELEPHONE BOOTH. In older phone booths, the receiver and microphone cap can be unscrewed and a small message inserted. Placing a small piece of plastic (such as part of a plastic sandwich bag) up inside the coin return slot can be used not only to temporarily store a message, but also to keep change from being returned to callers who get no answer or a busy signal. Good guerrillas can always use extra change. The plastic cover of the phone book allows a fairly thick text message to be inserted in the spine of the book.

2. NEWSPAPER VENDING MACHINE. If minimal time is involved in the exchange, the front newspaper that displays the headlines can have a message inserted in its pages when the drop maker purchases another paper. The coin return slot can also be used in the same manner as the phone.

3. GROCERY STORE. Placing the message or item behind a food display is useful. Also consider taping it underneath shelves or inserting it into specific packages. Be alert for security personnel if your approach appears to be clandestine; you may be suspected of shoplifting.

4. WALKING THE DOG. When taking an animal for a walk, there are constant and irregular "stops" along the way. The animal can be encouraged to sniff around a specific drop point while you appear to wait impatiently.

5. MAINTENANCE POINTS. A paper towel dispenser in a public rest room, the vacuum cleaner dust bin at a car

wash, or the underside of a metal shelf inside a janitor's closet are all examples of maintenance points that can be used as dead drops. Though access is often limited to the person responsible for maintenance, these locations are frequently left unsecured. A document sealed in a plastic bag and placed inside of a liquid soap dispenser in a rest room is a good example.

6. PUBLIC TRANSPORTATION. For short-duration drops, a city bus is excellent. The sender gets on and places a small message under a seat panel, among advertisements posted along the upper walls, or in a bus schedule bin. Within minutes, the receiver gets on the bus and retrieves the message.

Public transportation such as trains, taxicabs, and buses can also perform a unique courier service for a cellular operation, functioning as a sort of "mobile drop." A European terrorist group employed the same taxicab for all of its basic transportation needs, sometimes leaving messages and even funds for cell members in the backseat cushion. The cab was called by number to pick up cell members at various places throughout the day.

7. FIXTURES. Any item that is accessible and permanent can be used as a dead drop. Vending machines, plant holders, lamps and candle holders in restaurants, and so on are all good drop fixtures.

8. REFUSE. Any item that is normally considered garbage or litter can be employed in a dead drop plan. An empty cigarette pack crunched up and left at a specific location is a common KGB and GRU tactic. Empty soda cans used to be employed extensively; however in today's "environmental awareness" era, aluminum cans will be picked up for recycle if "dropped" by an agent. A certain wastebasket, Dumpster, or bin can be the drop location.

The advantage of refuse is its commonality in many areas, as well as its "untouchable" nature. Most litter is almost invisible to ordinary perception. In fact, many peo-

ple cannot recall a specific piece of litter on the ground during a walk through a park. Thus the operative can place a specifically labeled wrapper or container in a fairly obvious spot and, unless the litter itself has value (such as an aluminum can) or the area of the drop is regularly policed by groundskeepers, it is actually quite secure.

9. MAGNETIC CONTAINERS. These can be made or obtained from any hardware or discount store. Small magnetic key boxes can store one page of text and can be attached quickly and securely to the underside of vehicles, restaurant tables, telephone booth ledges, etc.

10. LIBRARIES. Libraries are among the best dead drop locations. An operative can check out a book, place a message carefully in the cover or along the spine, and return it to the book depository. He then instructs the recipient to check out the book in a day or two, after it has been placed back on the shelf. (Looking in the back of the selected book will indicate if it has been checked out recently.) Old or obscure books located high or low on the shelves are ideal for these transfers. The microfilm and card catalog drawers are also quite suitable, as are the magazine archives, library furniture, and rest rooms.

The above are only examples of possible dead drops. Use your imagination and create a list of several locations. Assess each one and select the best and an alternate. Consider your life-style and normal routine as a contributing factor. *It is bad form to alter your life-style to service a drop.* It will be recognized by the opposition immediately for what it is.

Current technology has created other types of dead drops that are useful alternatives to physical or visual communications. The *electronic mailbox* concept is probably the most prevalent means of secure information exchange when a high degree of isolation and anonymity is needed. Computer bulletin boards, telephone mailbox transfers, automated fax systems, and ordinary answering machines have much potential in this regard.

Discussions of these technologies and their applications can be found later in this book.

Message-Received Signal

When the operative has completed the cycle and picked up, or *serviced*, the drop, a means of advising the sender that the message was received is the final component in the process. The *message-received signal* can be as simple as a mark on a wall, such as crayon or chalk graffiti, or more complicated, such as the absence of an ornament normally hung over the rearview mirror of a vehicle parked on a busy side street.

The message-received signal is vital to the physical security of the drop. If the sender does not receive the signal within a reasonable amount of time, he must conclude that the drop has been burned for one reason or another and go to a prearranged backup plan.

The trainee should be advised that message-received signals are the only means of ensuring that the opposition has not stopped the drop process. Yet the Farm instills in each trainee that although the signal indicates that the process was completed, it is by no means a reliable indicator that the drop has not been compromised somehow. The opposition may have intercepted the material, copied it, and replaced it, or the drop may have been placed under surveillance by the opposition. The message-received signal simply indicates to the sender that the receiver did service the drop and has received the message.

Live Drop

When an operation is facing an active OPFOR, it is frequently under alert surveillance. The content of the visual message must be kept away from the opposition, and the actual physical security temporarily lost during the dead drop process sometimes is not acceptable. In this instance, a person can be employed as the exchange

medium. The individual who serves as a conduit for information, either knowingly or unwittingly, is known as a *live drop.*

A live drop can be a bartender at a favorite watering hole, a barber, or a local deliveryman. He may know the content and purpose of the message, although this is quite rare. A live drop usually is an unwitting participant in the message transfer. If he is a willing participant, then he needs to have a duress warning signal to warn operatives of any danger.

CIA career trainees are advised that the use of a live drop generally is not a good idea. Although the right conditions may exist for the clever application of this technique, it is not as free from surveillance as it may appear, and the physical security of the message is limited to the physical security of the individual serving as the drop. This approach is also open to an infinite number of random risks and potential problems that are impossible to predict.

Message signals are employed in the same manner as with a dead drop. This helps ensure *operational security* (OPSEC) and also eliminates the need for both the sender and receiver to keep a level of surveillance over the live drop.

Brush Pass

The *brush pass* offers the greatest amount of physical security for a message transfer. An agent or representative casually brushes against another person and places the message in his hand or pocket. It requires significant practice to perform properly. This excellent transfer means keeps any sensitive message in the hands of the operatives only—it is not left anywhere or with anyone.

CIA trainees are drilled extensively in both the use of this technique and the methods of teaching its basics to potential operatives. The message signals are similar to drop servicing, though there is one other signal employed. When the brush pass is about to take place, the

sender must have a means of advising the receiver that the pass is safe to attempt. This signal is something that is present, such as a pen in a specific pocket. If the signal is not there, it warns the receiver that the sender suspects surveillance or is under duress.

The receiver of the message must also have a signal to indicate to the sender that it is "clear" to attempt the exchange from his point of view. The warning, termed the *abort* message signal, could be the absence of a newspaper or a watch turned around on the wrist. It is very important.

The brush pass has some hidden dangers that must be carefully assessed. For instance, in many urban areas certain drug transactions are conducted using a covert hand-off similar to the brush pass technique. In their refined mode, brush passes often appear to be some sort of pick-pocketing, which may alert a plainclothes officer trained to observe such activity.

Eye contact must be avoided during a brush pass. Heavy, unidentifiable crowds are present in most brush-pass scenarios, and although crowd behavior in many countries is predictably disinterested and detached, a trained observer will almost always be able to detect a brush pass taking place.

The most significant problem of using the brush pass is the amount of training and practice involved with teaching certain types of "agents" (such as a hotel maid or an employee of a target company) the technique to transfer information for two operatives. CIA trainees are given numerous case histories where the brush pass was employed as a security precaution and went bad because of the random observer or unpredictable scenario occurring.

The brush pass has its advantages and limitations. With careful and constant practice, the operative can employ this ancient technique in certain situations with success.

APPLICATIONS FOR VISUAL COMMUNICATIONS PLANNING

The communications officer can employ the visual communications exchange as integral components of any underground network. The basic features of visual exchange are security, bulk message transfer capability, and low-technology hardware requirements. The fundamental problems most encountered are complexity of routine, slow process of exchange, and intensity of training required for all participants. Each individual COMMO net has capabilities and limitations in employing visual communications.

Command Net

The need for complete understanding of operational instructions as well as a multilayered isolation from all cells tend to make visual communications highly useful in delegating authority and sending clear orders. Slow process can be a problem.

INTEL/OPS Net

This network requires the most anonymous and most reliable means of communication available. Intelligence personnel often need to transfer detailed reports and photographic and image documents, as well as receive multipage tasking assignments. Speed is a significant problem in the operations section.

Action Net

There are severe limitations for internal use of visual communications with this network. Although command can provide instructions using this media as well as activate "sleeping" units quite effectively, the need for rapid communications that are difficult to intercept or trace requires voice communications (see Chapter 7). Action cells are composed of physically tough, highly trained,

teamwork-oriented specialists. It is generally the most interdependent cell, and its internal COMMO network reflects this. Speed and reliability are the most vital aspects of the communications plan for this element.

ADMIN/LOG Net

For administrative purposes, visual communications are useful but limited. Document control and potential for security leaks frequently make visual communications impractical. Additionally, in many underground cells the administrative and logistics network is made up of sympathizers, indigenous members of the local population, and more "mainstream" population segments who are only part-time participants in the underground operation and seldom active in any incriminating capacity. Therefore, this network requires a less covert method of communications that allows it to quickly open and close down safehouses, transfer funds and materials, and otherwise participate without any trace of the participation.

Overall, visual communication requires a level of training and practice to be effective. It is an excellent medium for covert intelligence ops but is less useful in fast-paced direct actions. Visual communications exchange procedures are well-suited as a primary means of running agents, and make excellent alternate or backup systems for deactivation and abort commands.

5 ● BULK TEXT MESSAGE PROCESSING

After teaching the basic methods of message transfer using physical means, the CIA training program focuses on the process of miniaturizing messages and documents. Methods such as tiny camera applications and the use of microfilm and microdots are explained.

Unfortunately, many operatives do not have access to such sophisticated "spy toys" and hardware. This chapter will discuss alternative means for condensing text messages using ordinary devices.

IMPROVISED MICROFILM

In many underground operations, there is a need to transfer a large amount of text information. Intercepted log sheets, detailed biographical data on a target or opposition member, operational details for a mission, and so on can sometimes entail hundreds of pages of text.

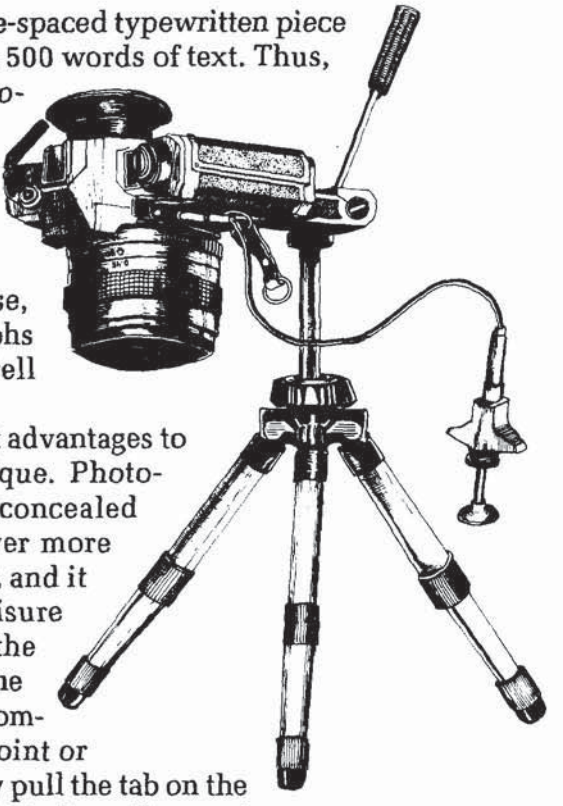
The following technique is simple, reliable, and capable of condensing more than five hundred pages of typewritten text and illustrations into a package smaller than a pack of cigarettes.

An ordinary 35mm single lens reflex (SLR) camera is purchased new or used. Most low- and medium-priced 35mm cameras come with a standard 50mm lens.

Four 8 1/2 x 11 sheets of typewritten text are placed on the floor and the camera is focused to get a sharp image from approximately 4 feet. Using ordinary slow-speed black and white film, the operative photographs four sheets per frame. A bright desk lamp is a good light source. (The standard flash attachment tends to produce a bit of glare on the page.) After some practice, one can condense a detailed typewritten report into a small package very cheaply.

For example, a single-spaced typewritten piece of paper can hold about 500 words of text. Thus, 2,000 words can be processed on each frame. A 72,000-word document, or 144 pages of text, can be processed on each 36-exposure roll of film. Of course, drawings and photographs can be transferred as well using this technique.

There are significant advantages to employing this technique. Photographed text can be concealed from the casual observer more easily than bulky paper, and it can be developed at leisure by the recipient. If in the process of transferring the roll of film the agent is compromised at the drop point or in transit, he can quickly pull the tab on the roll and expose the film. Perhaps the most notable aspect of this approach is the fact that the operative can get his own equipment and conduct this technique with minimal training or supervision.



35mm camera set up to shoot improvised microfilm from text sheets. (Illustration courtesy of Mark Camden)

If improvised microfilm is detected or discovered, the content will be considered some sort of espionage message. Fortunately, 35mm cameras and film are common worldwide and quite normal in appearance. Black and white film can be developed quickly using an inexpensive home darkroom, thus eliminating the need for outside photo processing.

Improvised microfilm is probably the most secure and reliable technique of transferring visual information via the dead or live drop or brush pass. Two rolls of film can fit inside of a cigarette pack and can contain 288 pages of single-spaced typewritten text, which is the equivalent of 576 pages of double-spaced text.

For many types of text, four pages per frame can be enlarged with a fair degree of image resolution. Yet there can be problems with putting this much text onto each frame of 35mm film. The fundamental problem is the need for exacting photo processing by the recipient of the film. Additionally, the individual taking the photographs must have a steady tripod and an excellent source of light. Since it is not always possible for the individual taking the photographs to be particularly skilled, nor is it likely that he will have an opportunity to review his handiwork, an alternative method should be considered for the relative neophyte.

As a communications officer for an underground unit, it may be better to instruct an operative to simply photograph one page of text per frame, and to carefully monitor the quality of the text. It is important to keep things to a basic level of skill that any member of any cell can use effectively with a great deal of confidence.

As a result of a 1982 FBI sting operation, our Soviet friends were kind enough to unwittingly provide a document outlining photographing techniques for a "neophyte" operative. Their military intelligence apparatus GRU (Glavnoe Razvedyvatelnoe Upravlenie) is very aggressive in the Washington, D.C., area in its attempts to

collect any morsel of useful information about U.S. military capabilities. The activities of the Pentagon are, of course, the highest priority target for the GRU.

Agents assigned to military attaché duties at the Soviet Military Office (SMO) at 2552 Belmont Road in northwest Washington are expected to "work" the metropolitan area continuously, collecting tidbits of military information at trade shows, public access areas, and even in bars and restaurants. GRU intelligence personnel are well trained and have had a number of successful penetrations of critical U.S. military operations.

What is interesting is the fact that instead of aggressively focusing activities on high-level U.S. military personnel, the Soviets seem to specialize in the development of lower-ranking military and civilian employees of the Department of Defense (DOD) as sources. These clerks, secretaries, and radio operators are "spotted" by GRU agents, and a number of methods are employed to determine their vulnerabilities. If, for instance, a radio operator is in a financial bind, a GRU agent may pose as a member of the intelligence agency of a third nation and pay for what would appear to the victim to be fairly "harmless" information for the legitimate needs of a nonhostile foreign power (as is often represented by the GRU agent).

Another good source of information for the GRU is, in fact, "walk-in" business, where a low- or mid-level U.S. military contractor or soldier simply visits or somehow contacts the Soviet military and offers services for a fee or some other consideration. The FBI counterintelligence division squad, CI-3, maintains constant surveillance on the SMO building for this very real threat.

Because the Soviets are successful with low-level DOD employees, GRU agents are versed in training the average American citizen in a variety of basic covert communications. The obvious method for spying on one's country is to collect classified documents or equipment and secretly transfer them to the paying

DEAR JIM (MAY I CALL YOU SO)
THANK YOU FOR YOUR NOVEMBER VISIT AND YOUR PARCEL. ALL THE DOCS ARE VALUABLE. I HOPE YOU AGREE THE MONEY YOU RECEIVED COVERS YOUR EFFORTS AND GOOD START. I THINK WE WILL CONTINUE OUR MUTUALLY BENEFICIAL BUSINESS. I WILL DO MY BEST TO INSURE YOUR SECURITY. PLEASE DO THE SAME ON YOUR PART.
ALL NEXT REWARDS - ACCORDING TO THE VALUE OF THE DOCS.
SORRY FOR THE COMPLICATED WAY OF OUR FIRST TRANSECTION. YOU UNDERSTAND IT WAS DONE ONLY FOR SAFETY REASONS.

IN OUR FURTHER COOPERATION I RECOMMEND YOU THE FOLLOWING:
- KEEP TRYING TO COLLECT UP TO DATE, COMPLETE, WITH HIGHEST CLASSIFICATION DOCS AND KEEP THEM AT HOME OR IN ANY SAFE PLACE YOU CHOOSE.
- THE BEST WAY TO COPY THEM IS BY CAMERA. I ENCLOSE ADDITIONAL $ 400.00 FOR THAT PURPOSE AND RECOMMEND YOU TO BUY AT THE W. BELL & CO AN "OLYMPIC OM-IM" WITH f/1.4 LENS. USE WHITE &BLACK CODAK FILMS "PANATOMIC -X, 52 ASA". TO MAKE A COPY OF GOOD QUALITY BY SURE TO FIX FOCUS AT A DISTANCE NOT MORE THAN 18-20 INCHES.LIGHT - 1 TABLE LAMP X 100 WATTS. BEFORE SHOOTING A DOCUMENT MAKE SOME CONTROL SHOOTINGSOF ANY OTHER SIMILAR TEXT. DEVELOP YOURSELF AND CHECK IT. IF STILLS ARE O'K, START SHOOTING DOCS. KEEP THE FILMS UNDEVELOPED IN CASSETS IN A SAFE PLACE. BUY FILMS IN DIFFERENT STORES.
- OUR NEXT TRANSECTION WILL BY IN APRIL. PREPARIED STUFF (FILMS OR COPIES) WRAP INTO WATERPROOF PACKAGE PREFERABLY IN A BLACK PLASTIC GARBAGE BAG.

PUT THE PARCEL IN PLACE #1 (SEE DESCRIPTION). IF BY ANY REASON THE USE OF THIS PLACE IS DIFFICULT USE PLACE # 3 (RESERVED). THAN GO TO THE PLACE OF MEETING # 4 AND BE SURE TO ARRIVE AT 8 P.M. WAIT FOR 10 MINUTES. IF I FAIL TO COME GO TO THE PLACE # 2 AND PICK UP MY PARCEL. IN CASE THERE IS NO PACKAGE IN # 2, CHECK # 3. AFTER PICKING UP MY PARCEL PUT A SIGNAL AT A PLACE # 5. THAT WILL BE THE END OF THE TRANSECTION.

IN MY PACKAGE YOU WILL FIND FURTHER INSTRUCTIONS. REED THEM AND FOLLOW THEM CAREFULLY.
- FOR THE SAKE OF SECURITY OUR MEETINGS OR EXCHANGE OF PARCELS WILL TAKE PLACE NOT MORE THAN FOUR TIMES A YEAR. THE MORE DOCS YOU COLLECT IN FILMS THE HIGHER WILL BE REWARD.
- IF BY ANY REASON WE FAILED TO MEET OR MAKE AN EXCHANGE COME AT 8 P.M. ON LAST SATURDAY OF EVERY MONTH COMMENCING MAY TO THE PLACE # 6. IN THIS CASE YOU WILL MEET ME OR ONE OF MY FRIENDS. PLEASE FOLLOW ALL INSTRUCTIONS GIVEN IN DISCRIPTION OF #6.
- DO NOT TRY TO CONTACT ME BY ANY WAY. IF EVERY MEANS OF COMMUNICATION MANSIONED ABOVE ARE CUT IT WILL BE MY DUTY TO FIND THE SAFIEST WAY OF GETTING IN TOUCH WITH YOU.

AFTER USING ## 1, 2, 3, 4, 5 DESTORY THEM AND KEEP # 6 ONLY.
- BE CAREFUL AND WISE NOW AND IN THE FUTURE WITH THE SPENDINGS.
- MAKE NECESSARY NOTES TO REMEMBER AND DESTROY THIS MESSAGE.

WISH YOU THE BEST.

YOUR FRIEND NICK.

Reproduction of an FBI photo of GRU letter outlining steps for document theft and delivery.

agent. The Soviets are fairly adept at this activity, keeping dozens of CI-3 agents busy monitoring the activities of GRU personnel.

An FBI sting operation known as Operation Jagwire was carried out in 1982 when a civilian research contractor for the Pentagon was used as a false walk-in to the SMO. The Soviet GRU officer took the bait and gave written instructions to the contractor on how to use an ordinary 35mm SLR camera to take good quality photographs of documents without arousing any suspicion.

As can be seen in the document, the Soviets employ the improvised microfilm approach to stealing documents, and they advise not only the model of camera to be used but also the type of film. The recommended "Olympus OM-IM camera with fw1.4 lens" essentially is an ordinary 35mm SLR camera with a stock 50mm lens. Although the recipient of this letter was an FBI plant, it is interesting that this single-page document not only offers encouragement to the GRU's new agent, but also outlines the simple method for document theft and provides a somewhat sophisticated communications plan employing a series of dead drops and signals.

PHOTOSTATIC REDUCTION

Many modern photocopiers have a feature to enlarge and/or reduce an image. This allows the operative to reduce the bulk of a text message to a more manageable size. In order to get a good image from the reduction, the copier must be of fairly good quality and have been serviced recently.

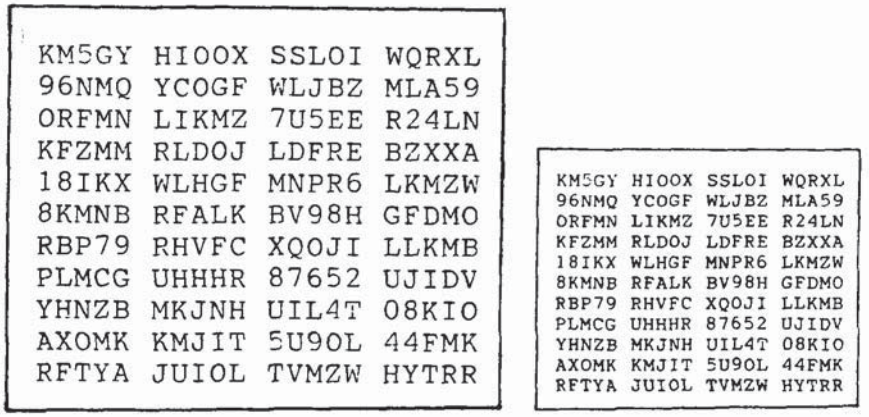
Text reduction via photocopier is useful if the following factors are considered and compensated for:

1. IMAGE DEGRADATION. If the copier is not of good quality or needs servicing, the image reduction is degraded. Normal-size copies may not be affected by poor resolution, but when text is reduced, subtle shades and other

signs of poor reproduction can be detected. You can frequently fix this problem by darkening or lightening the adjustment control on the front panel.

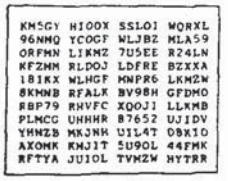
2. IMAGE REPROCESSING. Up to 75-percent reduction is realistic with most commercial copiers. What must be considered is that there will be an enlargement of the text on the other end of the message pipeline. This will, of course, be an enlarged "copy of a copy." Thus the quality of the copy machine on both ends of the process is important.

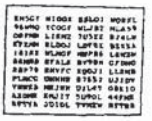
3. SPECIAL IMAGE PROCESSING. Opaque screen sheets are now available that can be of great help in diffusing the image of a reasonable-quality black and white photograph. These inexpensive plastic overlays are available in graphic arts supply stores. They put tiny dots over the photo image that help diffuse it, making it much easier to copy a recognizable end product. The overlay is particularly useful for aerial photographs and photos of buildings.


KM5GY HI0OX SSLOI WQRXL
96NMQ YCOGF WLJBZ MLA59
ORFMN LIKMZ 7U5EE R24LN
KFZMM RLDOJ LDFRE BZXXA
18IKX WLHGF MNPR6 LKMZW
8KMNB RFALK BV98H GFDMO
RBP79 RHVFC XQOJI LLKMB
PLMCG UHHHR 87652 UJIDV
YHNZB MKJNH UIL4T 08KIO
AXOMK KMJIT 5U9OL 44FMK
RFTYA JUIOL TVMZW HYTRR

KM5GY HI0OX SSLOI WQRXL
96NMQ YCOGF WLJBZ MLA59
ORFMN LIKMZ 7U5EE R24LN
KFZMM RLDOJ LDFRE BZXXA
18IKX WLHGF MNPR6 LKMZW
8KMNB RFALK BV98H GFDMO
RBP79 RHVFC XQOJI LLKMB
PLMCG UHHHR 87652 UJIDV
YHNZB MKJNH UIL4T 08KIO
AXOMK KMJIT 5U9OL 44FMK
RFTYA JUIOL TVMZW HYTRR

Example of text reduction by a standard photocopy machine. The text can still be readable, yet small enough to fit underneath a postage stamp.





Photocopy reduction of bulk text is not as effective as the improvised microfilm technique, but it is suitable as an expedient method. When using this approach it is important that the reduction process be followed with a test enlargement so that the sender is assured that the quality of the product is suitable for the receiver to enlarge and read.

6 ● GUERRILLA CRYPTOGRAPHY

Communications security (COMSEC) is a serious aspect of covert communications. COMSEC entails every active measure to deny unauthorized access to communications. It includes authentication procedures, physical security measures such as the use of drops, miniaturization of text, and cryptography.

Cryptography is the art and science of communications security. While covert operations require a secure means of transferring plain-text messages, there must also be built-in safety measures to defeat the OPFOR's ability to understand the message should it intercept the message anyway. This chapter will focus on some easy-to-employ options for encoding or encrypting text.

There is a difference between a code and a cryptogram. Both can be employed in underground communications, but the application of each is dependent on specific needs. A *code* is a prearranged group of symbols or characters that represents plain-text messages. It describes specific aspects of the operation in a manner that denies the OPFOR access to the content of the message. Coding standardized or frequently used words, names, or messages contributes to brevity, security, and understanding. For example, a team member, opponent, or target can have a code name. A situation or a condition can have a code word.

Encryption is the random, unintelligible conversion of a plain-text message. In an underground operation, the process of encryption must be fast, reliable, and secure. The coded product is termed a *cryptogram*. Although the term "code" has a different definition than "cryptogram," the term "encoding" is generally meant to define the process of deceptively altering the content of a plain-text message by using a *cipher system*.

There are two types of cipher systems used in military and intelligence operations. *On-line cipher* is an electronic method of encoding a message that is part of the transmission system. A voice scrambler, for example, is an on-line device. *Off-line cipher* is a method of encryption that can employ any number of transfer devices, including radio, visual, or wire. This section will cover off-line cipher techniques.

Since the use of *any* code or cipher is somewhat incriminating, the first step in developing a text message COMSEC plan is to make the enciphered text appear to be quite normal. One means of doing so on an expedient level is known in tradecraft as *document insertion*.

DOCUMENT INSERTION

As is stressed throughout this book, all aspects of covert or underground communications should be designed to appear to be quite normal in content and process. The act of transfer should not betray itself. The act of encryption must follow the same rule.

One important aspect of COMSEC is that the operative should use a variety of means and methodologies to exchange information. This approach tends to further deny the OPFOR the capability to intercept and understand the message. Document insertion—placing an encoded message within the text of a normal document such as a newspaper, magazine, or book—is an age-old technique that employs several active measures in COM-

SEC and is probably the most secure expedient method of underground text-message transfers.

For example, if the local library is used as a dead drop, the text message can be encoded with a one-time pad (more on this later) and the actual message inserted among the letters and characters on a specific page in a specific book. This multilevel approach is simple to employ and quite secure.

The following techniques are useful in document insertion.

Character Marking

A sharp pencil can be used to carefully mark the desired characters on a printed page. "Pencil lead" is actually graphite. Although it has a dark gray image when pressed down on paper, it cannot be easily detected over the black indelible ink of a printed book's letters. However, when a marked page is held at an angle to fairly bright light (such as used for reading and common in a library), the characteristic "shine" of the graphite markings on the characters is quite obvious to the naked eye.

There are intrinsic security features to this approach. No physical security precautions need be taken for possession of an ordinary pencil, and once the receiver has copied the message, it can be erased.

A black or blue pen can be used for character marking with fairly good results. The ink also tends to "shine" under light, although it cannot be erased as easily as pencil. Ink markings can be used for throwaway transfers using a newspaper or magazine.

One unique and considerably secure tool for character marking is the ultraviolet (UV) pen. This is a marking pen used to invisibly mark property, such as stereos and televisions, for security purposes. Under an ordinary black-light bulb, the ink is quite pronounced. UV pens are available in many department stores and are often

given away free by police departments and community watch groups in the United States and Europe.

Though somewhat elaborate, the most significant advantage of the UV pen is that it is considerably faster than the tedious method of slowly and carefully marking the text with a pencil or pen. The disadvantages of UV pen use are the obvious intent if caught marking text with one and the fact that the message cannot be erased from the page.

Secret Writing

The UV pen employs an age-old technique known as *secret writing*. Secret writing was used for centuries as a means of communications. A variety of substances have been used as invisible ink, from sophisticated chemical compounds to milk and even urine. The essential qualities of secret writing are that the message be inserted into an innocent document and the means of reading the message be reliable and secure.

Secret writing is seldom used anymore because chemical analysis of paper is now fast and reliable. It has some use for POWs or prisoners, but again, it is not the wisest approach. It is normally employed only against the most naive or unsuspecting opposition. For example, in Nazi Germany the feared SS (Shutzstaffel) used secret writing on the back of paper ballots to determine how certain Nazi party members voted on various referenda. Ordinary milk was used to number the back of each ballot. When dried milk is exposed to low heat, the markings turn brown and show up easily. The marked ballots were simply run across the heat of a candle or hot plate, and the numbers were easy to distinguish.

Pin-Puncture Marking

Other more innocuous measures of low-profile document insertion are simpler and much less suspicious, simply because there is no need for special "invisible

ink" pens or processing materials. It is impossible to overemphasize the inherent risks of having any type of "spy paraphernalia" in your possession.

Probably the fastest method of reliable text marking is an ordinary straight pin or needle. The letters are marked with the pin point by carefully puncturing each character. Close scrutiny of the text will not reveal the message until it is held up to light. The pin puncture technique can be employed with newspapers, magazines, or any publication that can be burned easily after use. Because their "universal" nature makes their possession and use quite normal, a good choice is those free entertainment or TV-oriented pulp publications or independent newspapers that generate revenues through advertising. They are given away at newsstands and in grocery stores in most cities.

Document insertion can be used for SITREPS, command instructions, and warning orders, which are usually brief yet must be kept secure. Document insertion lends itself to dead drop and brush pass techniques quite well.

Typewriter "Lift-Off" Messages

A more advanced method of document insertion involves a correcting electronic typewriter. These typewriters have a "lift-off" correction ribbon in addition to the ordinary print ribbon. Many typewriters that have this feature also have full-line correction, meaning you can push one button or key and remove the word you just typed or any word typed on the current line. Full-line correction has an unusual characteristic that can be employed in document insertion.

The correction ribbon makes an impact on the page that cannot be erased. In fact, it is easier to erase the black typed image than it is to remove the white correction image. If you type a line on a typewriter with the lift-off ribbon and then use the full-line correction feature to lift off the entire line, it is still readable under good light (if nothing else is placed over it). By typing a "normal" dou-

ble-spaced letter and inserting your encrypted text every other line between the visible text, you have a fairly secure means of message transfer. To increase security, you can type your hidden message in this fashion on the back of the page of "normal" text.

This approach can also be used with illustrations, although your text must "work around" the black lines of the artwork, since the correction ribbon will white them out. Another useful method of employing the correction feature is to take an ordinary envelope apart and type the message on the inside. Reassemble the envelope, put your "normal" message inside, and send it.

Overlay Technique

Probably the most secure means of document insertion is known as the *overlay* technique. The overlay technique employs a separate sheet of paper with holes or markings on it that allow the operative to decode the actual text message. For instance, a page of an article, book, or letter is used as the medium. The operative has in his possession a sheet of paper that has holes punched through it with a paper punch. When the paper is placed over the page, the other letters in the text are covered and only the actual message can be read.

For 8 1/2 x 11 pages, the hole punch process can be duplicated with an ordinary pin. For example, the operative sends a multipage document to the receiver. One of the pages has pinholes in it. When the holes are punched through, one or more predetermined pages contain the desired message.

Physical security is important with the overlay technique. Possession of an unmarked piece of paper with holes punched in it is very incriminating. For certain applications, however, this method of document insertion is extremely secure and may be worth the risk. As seen, the size of the holes in the paper can be

quite small—the actual characters don't have to be legible so much as the holes have to be big enough to locate reliably.

IMPROVISED ONE-TIME PAD

Although covertly arranging the need to conduct a message transfer, establishing a method of exchanging the traffic, and inserting the message in an ordinary document all contribute to a high degree of COMSEC, the above methods of tradecraft are intended more to protect the physical security of the transfer and the identity of the operatives than to actually keep the *content* of the message secure from the enemy. What is needed at this point is a means of completely encoding the plain-text message such that it is extremely difficult for the OPFOR to decode.

No code is "unbreakable." Modern supercomputers can analyze and study literally every possible combination available in an encrypted message and determine every possible message. This is no easy task. For instance, if one word in an encoded message has five characters in it, the computer system must use several means of "attacking" this "word." The obvious way may appear to be by simply using its memory and speed to create a list of all five-letter words.

There are several flaws in this seldom-used approach. First of all, the computer does not know if the five encoded characters are indeed a "word" at all. They may be an abbreviation, a transposed number, or a word from a different language. Second, since there are twenty-six characters in the English language, to create a list of all combinations of five characters would require a tremendous amount of memory and time. The number of possible words that can be created out of a five-character group can be determined by using the following formula:

A = NUMBER OF POSSIBLE CHARACTERS (26)
B = NUMBER OF CHARACTERS IN WORD (5)
C = TOTAL NUMBER OF POSSIBLE COMBINATIONS

FORMULA $C = A^B$
OR $C = 26^5$ (26 x 26 x 26 x 26 x 26)
OR C = 11,881,376 possible combinations

Of course, there are not anywhere near 11.8 million five-letter words in the English language or, for that matter, any language.

The computer could quickly scan through this huge list of combinations and select only those combinations that were words in the language in question. The problem would be that the operator would then have a list of every possible word that the five-letter combination could be, yet still be nowhere near knowing which one.

The supercomputer can take a five-character group and analyze it using other criteria. The word must have at least one vowel, for instance. The "context" and location of the group can be considered. Although this approach sounds beyond the capacity of even a huge computer, it is done. The characters in each group are first analyzed by themselves and then as part of the whole message. Then the computer can make sentences and even paragraphs out of all of these encoded "words" and eventually come up with a manageable number of possible messages from the encoded text.

The point is that a supercomputer's memory can easily process hundreds of millions of random character combinations at once without human participation or error. Within seconds, this system can take a 200-word message and come up with a limited number of possible meanings for the encrypted text. The actual task for the cryptoanalysis computer is to come up with the *key* to the code. Once it has determined the content of the message, the computer can inform the operator what the actual key

is. It can also define the likely means by which the key was created.

In order for the covert operator to effectively approach the threat of an encrypted message being decoded, it is vital that he understand that 100-percent security is impossible. The success of any code is limited to the capabilities of the operatives, the time available, and the potential threat. A high-risk operation that is considered an active threat to U.S. national security can expect to have no reliable cryptosecurity because the degree of sophistication employed by the opposition to break the code will probably always succeed.

For less sensitive and dangerous activities, there is a means of encrypting plain-text messages that will severely task even the most determined cryptoanalysis team. This approach is termed the *randomly generated one-time cryptosystem.*

The most secure means of using a specific code key is to use the code only once. This means that every message exchanged between two parties must use an encryption method that changes daily, hourly, or on a per-message sequence. On-line encryption devices are designed to constantly change the characters of a plain-text message in sync with all other such devices in the "net." The underground off-line system must accomplish the same thing. A one-time cryptosystem that randomly changes the content of each message in a manageable form by constantly altering each character is extremely difficult to defeat yet quite simple to employ. The method most practical for this approach is the *one-time pad.*

A one-time pad is a small booklet of sequentially numbered sheets containing a randomly selected code key for each character and number in the language used. (This section will focus on the English language, but the approach can be employed with any other language just as easily.) When the operative wishes to transmit a text message, he writes the entire message on a piece of paper,

leaving space between each line for the code characters. Once the message is written out, the operative takes out the one-time pad and tears off the top sheet. He uses this code key to transpose the message into the encrypted form. Once finished, he destroys the one-time pad sheet by burning the page completely, stirring the ashes, and disposing of them carefully.

Possession of a one-time pad is extremely incriminating. An operative who is caught with one is generally in no position to disclaim a variety of charges. For this reason the physical security of the pad is critical. One approach is to make the pad as small as possible. This is quite easy. With twenty-six letters and ten numerals to consider in a typical message, the operative can make a one-time pad sheet the size of half a matchbook with no special tools or equipment. For example, here is the key sheet and code sheet for a one-time pad made on an ordinary typewriter using the twelve pitch setting:

Key sheet:

```
ABCDEFGHI
JKLMNOPQR
STUVWXYZ1
234567890
```

Code sheet:

```
V8PI4MKRC
3YFTBA6OW
DLJGE5ZQH
N0L9X2SU7
```

PLAIN TEXT = NEED FUNDS WIRED TO AGENT N5
CODED TEXT = B44I MJBID ECW4I LA VK4BL B9

Although the small size of the one-time pad is illustrated above, in actual use there are a couple of other considerations. This one-time pad is only a little bigger than the average postage stamp and is quite easy to conceal. You can easily create seventy code sheets on a single sheet of 8 1/2 x 11 paper. As long as you run it off on a copy machine (for the receiver), cut out each

small sheet, and attach them in sequential order of, say, seven sheets each, there is no need for you to sequentially number the individual sheets. Each tiny seven-page one-time pad can fit easily behind the matches in a matchbook.

Keeping the one-time pad small in sheet count is useful from an operational security and concealment standpoint. If each agent only has seven sheets in his possession, he can usually operate from one week to several months without requiring a replacement, depending on the number of messages he sends or receives.

The use of the one-time pad must also be carefully considered from a practical standpoint. Even though the message in the example cited above—NEED FUNDS WIRED TO AGENT N5—is encoded, it is actually relatively easy to break. The standard practices of cryptoanalysis would recognize three aspects of this encoded message—word content, word size, and word format—and break it within minutes.

Codebreakers would recognize that the six-word message has the character 4 in it four times; it is the character most often used in the encoded message. The most common letter in the English language happens to be the letter E, and 4 does, in fact, represent the letter E.

The fourth and fifth words in the message are only two characters long. There is a limited number of two-letter words in the English language. If the cryptoanalysis expert recognizes the format of this message as a sentence, he will probably deduce the fourth word as "to." After deducing the first word as "need" based on E being present twice, whatever is "NEED"ed has got to be described, and how and who to send it "TO" might also be included in order for the sentence to make sense.

To enhance the security of the one-time pad, a standardized means of creating text messages that will

defeat the cryptoanalysis process of recognizing word content, size, and format is required. This can be partially accomplished by using *groups* of uniform size. For instance, the message NEED FUNDS WIRED TO AGENT N5 can be written as NEEDF UNDSW IREDT OAGEN TN5. The last group is given two extra Qs to keep the group size uniform. Thus you have the following:

PLAIN TEXT: NEEDF UNDSW IREDT OAGEN TN5QQ
CODED TEXT: B44IM JBIDE CW4IL AVK4B LB9OO

This approach not only makes the codebreaker unable to employ format and word size analysis, but the addition of two random characters at the end of group five will also affect his ability to employ word content analysis to a degree.

Another practical consideration in even a small covert op is the need for the recipient to verify that he is using the correct one-time pad to encode and decode the traffic. In the coded message there should be one word group that identifies the pad used to send the traffic. This can be as simple as numbering each pad and sending that number encoded as the first word in any message, or by taking a certain section of the pad itself and sending that sequence of characters as the first (or last) group in the message.

For instance, in our example, the last five characters in the bottom column of the code are X2SU7. This can serve as the *code group identifier*, which confirms to the receiver of the message that this specific one-time pad has been used . . . and *also* has now been destroyed.

To create a one-time pad, simply write the entire alphabet and all ten numerals two times in two separate columns. Cross off the characters in the second (code-key) column as you randomly assign them to the characters in the first (plain-text) column. The sheet will look something like this:

A	R	1	A	X
B	8	2	B	2
C	J	3	C	3
D	1	4	D	4
E	U	5	E	5
F		6	F	6
G		7	G	7
H		8	H	X
I		9	I	9
J		0	X	0
K			K	
L			L	
M			M	
N			N	
O			O	
P			P	
Q			Q	
R			X	
S			S	
T			T	
U			X	
V			V	
W			W	
X			X	
Y			Y	
Z			Z	

Although you may feel confident in your ability to create a random one-time pad using this technique, after making several dozen you probably will see certain identifiable trends in your character assignments. Certain characters will tend to have only two or three character codes assigned to them every time. This process is difficult to explain; the human mind simply is not very good at creating random letters or numbers. This characteristic keeps the one-time pad from being a randomly generated one-time cryptosystem. Therefore, when assigning char-

acters, get in the habit of starting from various points in the columns. This helps your mind keep the system more random in nature, making it more difficult for the opposition to recognize any trends in your creation.

As a practical exercise, make a starter sheet as shown above and run off twenty copies on a copier. Then attempt to randomly assign a code-key character to each plain-text character on every sheet. Unless you start at different points (and for many people, even if you do start at different points), you will recognize the above phenomenon. If you are able to identify any pattern in character assignment, then a crytoanalyst should be able to do so too, and any cryptosecurity computer system certainly will be able to. Although this point sounds minor, it is worthy of careful consideration as you create your one-time pad. Don't overestimate your abilities or underestimate those of your opposition.

Computer Generation of One-Time Cryptosystems

Operatives who own or have access to a personal computer (PC) may want to experiment with creating a random series of alphanumeric characters. Although this approach sounds like it might be the ideal means of creating an unlimited number of secure one-time pads, there are some severe technical limitations to a personal computer that may not make this approach practical.

In most computer languages there is, in fact, a command for the random generation of a number or character. (In BASIC, this command is usually RND.) But this command only *appears* to generate a random string of characters. The PC can be instructed to create a list of all twenty-six letters and ten numerals in a "random" sequence without duplicating any character in the string. The problem is that if you run the program again on the same machine or even on a duplicate computer, it will generate the exact same sequence of characters more than 90 percent of the time. This translates out as a very unreliable approach to

random character generation because if it can be duplicated, a cryptoanalysis computer will recognize the pattern, know that the source for the one-time pad was a computer, and immediately break the code.

No personal computer is capable of creating a truly unpredictable random list of characters. The reason for this is not so obvious. Essentially, a computer has a clock circuit feeding into the actual brain of the microprocessor, the *Central Processing Unit* (CPU). The clock controls the speed and sequence of data as it passes through the CPU while being processed in the form of binary bits of data. When a BASIC programmable computer (such as the IBM PC and compatibles, the Apple, and most others) receives an RND code, the machine "selects" a character based on a predetermined and generally hardwired mathematical formula. Although the resulting character string may appear to be generated randomly, it is actually quite predictable in process. If a computer process is predictable, then it can be duplicated by another more powerful computer, which in this case means that it generates a breakable code.

There is another way to computer generate a pseudo-random string of characters that may have some merit. Most PCs employ a *Disc Operating System* (DOS) that accepts its own series of commands. The standard system on the IBM PC is the Microsoft disc operating system, known as MS/DOS. In MS/DOS BASIC, the command RANDOMIZE instructs the CPU to execute a random selection based on a number that the operator is prompted to enter. This number is used by the system to generate the random string.

The PC has an internal time clock that keeps track of days, hours, minutes, seconds, and hundredths of seconds. Accessing this clock in the CPU requires the MS/DOS command TIME$. If the machine is instructed to create a random selection based on the current time, it will create a list of characters by constantly updating the

actual time on its internal clock, which changes one hundred times per second. The RANDOMIZE TIME$ command is perhaps the most workable selection criteria for a one-time pad. (In ordinary BASIC, the TIME function command variable is TI$.)

The problem with this approach is that the character string generated will have certain patterns identifiable by a more advanced computer, such as the CRAY II at the National Security Agency (NSA). If the CRAY II detects or suspects that random generation took place on a PC system, its huge memory and high-speed clock will eventually determine the initial TIME$ variable used to generate the first string and every subsequent string. Once the initial TIME$ variable is determined, it can be entered into a similar format MS/DOS PC system and the "random" character string will be duplicated. Although the OPFOR would be required to go to elaborate means and utilize advanced computer cryptoanalysis to break this code, it could be done. The point here is that true random generation is actually beyond the means of current PC technology.

As should be obvious, the ability to create a random group of characters in a random order is fairly easy for the human mind to do on a somewhat unpredictable basis. With practice, this work can be done by the brain much better than most computers.

Although random selection is generally beyond the capabilities of the ordinary PC, it is one of the basic characteristics of a recent technology known as *artificial intelligence*, or AI. AI is the process where a computer system can perform such abstract tasks as "creative decision making" and "learning" somewhat emotionally based concepts such as morality. Random selection in an AI system relies on a series of complex mathematical formulas that provide the computer with factors that are similar to the human thought process.

Essentially, a random character string generated by a computer with AI architecture and software is made by

random generation of a mathematical formula, which is then used to randomly generate a character. The process continues with different formulas for each character and each string of characters. Because of the nature of the process, the system cannot duplicate character strings. Unfortunately, an AI computer system is currently beyond the realm of the typical underground operative.

The most significant advantage of computer generation of a one-time pad is speed. With practice, manual one-time pad generation can be accomplished in about five minutes, including transcribe time. Yet a high volume of one-time pads may be required as an integral part of a particular communications plan. To manually create a list of seventy different one-time pads would take about six hours plus the time required to process and package them. This time estimate may be quite conservative, however, as many people would have a great deal of trouble making up seventy completely different one-time pads.

Because of the inherent difficulties and time-intensive nature of random one-time pad generation, the author decided to locate someone who could take into account the known vulnerabilities of the IBM PC and somehow develop a simple program that would quickly generate a large number of different one-time pads.

The computer software development community is made up of professional analysts and college-educated specialists, as well as an impressive number of gifted "amateurs." Some of these amateurs are known as *hackers*, a somewhat clandestine and close-knit community of introverted and often nonsocial types who are suspicious of writers or anyone else who want to know about their skills.

After checking a variety of computer bulletin boards and private networks around Northern California's Silicon Valley as well as in the metro Washington, D.C., area, a uniquely qualified expert on the subject was located and found to be cooperative.

Kenneth W. Balch is a former air force intercept ana-

lyst who has been employed at a variety of National Security Agency (NSA) radio intercept posts worldwide. His job was to intercept and analyze coded continuous wave (CW, or Morse code) traffic generated from unknown sources around the world and attempt to identify its content. Monitoring radio Morse code traffic sent manually and by computer for several years, Balch developed a unique insight into the clandestine exchange of message traffic. (He now is a private consultant to large companies, providing turn-key software systems, computer security advice, and data processing integration services.)

After several interviews and informal discussions about the technical problem of making a PC act "randomly," Balch sat down at his keyboard and developed a program with some unique characteristics. The program uses a multilevel random-generation formula to create a mathematical command that the computer employs to create a mathematically random character string. It was a challenge that Balch spent many admittedly enjoyable hours "playing" with.

Knowing that his one-time pad program could be attacked and defeated by an advanced cryptocomputer system such as the CRAY II caused Balch to smile. He stated that the capabilities of the CRAY II were not to be underestimated, but if nothing else, he could make the CRAY II work very hard for a long time in order to identify any trends in a one-time pad that his program could generate in about five seconds.

The Balch program uses the TIME$ command in an unusual manner. In order for the computer to come up with a number, the operator enters in a specific time—such as the current hours, minutes, and seconds (or any time, for that matter)—in twenty-four-hour time. The program adds the hours to the minutes and then multiplies this figure by the seconds of the running time clock in the PC. This calculation changes every second and makes the computer recognize any one of 3,504 individual numbers

at any given second in time. This number is then used as the basis to RANDOMIZE the ten numbers and twenty-six English-language letters. Each character is selected one at a time using this multirandom process until all thirty-six are accounted for by the computer, at which time they are printed out in a matrix of nine characters by four rows, to be used in a one-time pad the size of a postage stamp.

The total time that this process takes on an IBM PC with BASIC MS/DOS is just under five seconds. Seventy completely different one-time pads can be created in about six minutes.

After subjecting the program to several thousand runs of one-time pad generations and then feeding them into a "trend analysis" software program, it was determined that there were *no identifiable characteristics* between any of the pads generated. Balch's program was capable of advanced mathematical text generation that was virtually impossible to duplicate.

A larger IBM system was given an opportunity to analyze this program and its results, and instructed to calculate the actual mathematical odds of another computer being able to duplicate just one pad. The chances for this happening were 170,141,200,000,000,000,000,000,000,000,000,000 to 1.

The following pages contain the Balch program. He has designed three different programs for the reader to use. Program 1 is the actual one-time pad program. Program II is a way for the operative to computer generate a one-time pad and then simply enter in the message for an automated process of encryption. Program III takes a specific one-time pad and decodes it from encrypted text back to plain text.

```
10    REM Random Generated One-Time Cryptosystem
20    REM Written by: Kenneth W. Balch
30    REM Copyright (C) April 1990
40    REM
50    DIM USED(100)
```

```
 60   INPUT "How many one-time pads do you want?";NUMB
 70   FOR RETRY=1 TO NUMB
 80   COL=1
 90   FOR A=1 TO 90
100   LET USED(A)=0
110   NEXT A
120   LET B=VAL(MID$(TIME$,1,2))
130   LET C=VAL(MID$(TIME$,4,2))
140   LET D=VAL(MID$(TIME$,8,2))
150   LET E=(B+C)*D
160   RANDOMIZE E
170   X=INT(RND(0)*90)+1
180   IF (X<65 OR X>90) AND (X<48 OR X>57)
      THEN GOTO 120
190   IF USED(X)=1 GOTO 120
200   LET USED(X)=1
210   LPRINT CHR$(X);
220   COL=COL+1
230   IF COL=10 THEN COL=1:LPRINT
240   DONE=0
250   FOR A=1 TO 90
260   IF USED(A)=1 THEN DONE=DONE+1
270   NEXT A
280   IF DONE=36 THEN 300
290   GOTO 120
300   LPRINT:LPRINT
310   NEXT RETRY
320   END
```

```
8MCG50ZV7
IEX1KBNPF
23WHQSRT4
OLYUA9JD6
O0ADX4R9Q
ZPS8UKJIE
FN16W2GT7
VLMH3CBY5
```

```
 10   REM Random Generated One-Time Cryptosystem
 20   REM Written by: Kenneth W. Balch
 30   REM Copyright (C) April 1990
 40   REM
 50   REM The difference between this program
 55   REM and the other is this one
 60   REM will allow you to type your message directly in the
 65   REM keyboard and
 70   REM will print your message in encrypted form using the
 75   REM cryptosystem
 80   REM created by the computer.
 90   KEY OFF
100   CLS
110   DIM USED(100)
120   DIM CYP$(100)
130   REM F=1
140   COL=1
150   FOR A=1 TO 90
160   LET USED(A)=0
170   NEXT A
180   LET B=VAL(MID$(TIME$,1,2))
190   LET C=VAL(MID$(TIME$,4,2))
200   LET D=VAL(MID$(TIME$,8,2))
210   LET E=(B+C)*D
220   RANDOMIZE E
230   X=INT(RND(0)*90)+1
240   IF (X<65 OR X>90) AND (X<48 OR X>57)
      THEN GOTO 180
250   IF USED(X)=1 GOTO 180
260   LET USED(X)=1
270   LPRINT CHR$(X);
280   F=F+1
290   CYP$(F)=CHR$(X)
300   COL=COL+1
310   IF COL=10 THEN COL=1:LPRINT
320   DONE=0
330   FOR A=1 TO 90
```

```
340   IF USED(A)=1 THEN DONE=DONE+1
350   NEXT A
360   IF DONE=36 THEN 380
370   GOTO 180
380   PRINT "Enter your message and I will encrypt it
      using this one-time pad."
390   PRINT "Press | to end (Shift \).
400   KEYED$=""
410   WHILE KEYED$="": KEYED$=INKEY$:WEND
420   IF KEYED$="|" THEN GOTO 830
430   F KEYED$="A" THEN KEYED=1
440   IF KEYED$="B" THEN KEYED=2
450   IF KEYED$="C" THEN KEYED=3
460   IF KEYED$="D" THEN KEYED=4
470   IF KEYED$="E" THEN KEYED=5
480   IF KEYED$="F" THEN KEYED=6
490   IF KEYED$="G" THEN KEYED=7
500   IF KEYED$="H" THEN KEYED=8
510   IF KEYED$="I" THEN KEYED=9
520   IF KEYED$="J" THEN KEYED=10
530   IF KEYED$="K" THEN KEYED=11
540   IF KEYED$="L" THEN KEYED=12
550   IF KEYED$="M" THEN KEYED=13
560   IF KEYED$="N" THEN KEYED=14
570   IF KEYED$="O" THEN KEYED=15
580   IF KEYED$="P" THEN KEYED=16
590   IF KEYED$="Q" THEN KEYED=17
600   IF KEYED$="R" THEN KEYED=18
610   IF KEYED$="S" THEN KEYED=19
620   IF KEYED$="T" THEN KEYED=20
630   IF KEYED$="U" THEN KEYED=21
640   IF KEYED$="V" THEN KEYED=22
650   IF KEYED$="W" THEN KEYED=23
660   IF KEYED$="X" THEN KEYED=24
670   IF KEYED$="Y" THEN KEYED=25
680   IF KEYED$="Z" THEN KEYED=26
690   IF KEYED$="0" THEN KEYED=27
```

```
700   IF KEYED$="1" THEN KEYED=28
710   IF KEYED$="2" THEN KEYED=29
720   IF KEYED$="3" THEN KEYED=30
730   IF KEYED$="4" THEN KEYED=31
740   IF KEYED$="5" THEN KEYED=32
750   IF KEYED$="6" THEN KEYED=33
760   IF KEYED$="7" THEN KEYED=34
770   IF KEYED$="8" THEN KEYED=35
780   IF KEYED$="9" THEN KEYED=36
790   IF ASC(KEYED$)=13 THEN LPRINT:GOTO 400
800   IF KEYED$=" " THEN LPRINT" ";:GOTO 400
810   LPRINT CYP$(KEYED);
820   GOTO 400
830   PRINT:PRINT:PRINT "Program end. One-time pad
      erased from memory."
840   CLEAR
850   END
```

```
BW2MQ14IF
G7NXU3TA5
6HDYZROKP
SC0V98EJL
```

```
U3Z F6 HIQ HFXQ 135 BNN 433M 25OTH36 H3 23XQ H3 HIQ BFM
   31 HIQF5 6O6HQX6
HIF6 F6 B HQ6H
```

```
10    REM One-Time Pad Decoder
20    REM Written by: Kenneth W. Balch
30    REM Copyright (C) April 1990
35    REM This program will DECODE messages generated
36    REM using a one-time pad or
37    REM using the Random Generated One-Time
38    REM Cryptosystem programs.
39    REM When the computer asks for a letter,
40    REM look up the letter on your one-
```

```
41    REM time pad and enter the letter that should be there.
42    i.e. if B is
43    REM an encoded A, when the computer asks for B
44    you would type A.
45    KEY OFF:CLS
50    DIM CYP$(50)
60    KEYED=0
70    PRINT "Enter letter for CODE letter . . ."
80    FOR RETRY=1 TO 26
90    PRINT "Letter ";CHR$(RETRY+64);
100   INPUT CYP$(RETRY)
110   NEXT RETRY
120   FOR RETRY=27 TO 36
130   PRINT "Number ";CHR$(RETRY+21);
140   INPUT CYP$(RETRY)
150   NEXT RETRY
160   CLS
170   PRINT "Enter coded message and I will decode it for you."
180   PRINT "Press | to end. (Shift \)"
190   KEYED$=""
200   WHILE KEYED$="": KEYED$=INKEY$:WEND
210   IF KEYED$="|" THEN GOTO 620
220   IF KEYED$="A" THEN KEYED=1
230   IF KEYED$="B" THEN KEYED=2
240   IF KEYED$="C" THEN KEYED=3
250   IF KEYED$="D" THEN KEYED=4
260   IF KEYED$="E" THEN KEYED=5
270   IF KEYED$="F" THEN KEYED=6
280   IF KEYED$="G" THEN KEYED=7
290   IF KEYED$="H" THEN KEYED=8
300   IF KEYED$="I" THEN KEYED=9
310   IF KEYED$="J" THEN KEYED=10
320   IF KEYED$="K" THEN KEYED=11
330   IF KEYED$="L" THEN KEYED=12
340   IF KEYED$="M" THEN KEYED=13
350   IF KEYED$="N" THEN KEYED=14
360   IF KEYED$="O" THEN KEYED=15
```

```
370     IF KEYED$="P" THEN KEYED=16
380     IF KEYED$="Q" THEN KEYED=17
390     IF KEYED$="R" THEN KEYED=18
400     IF KEYED$="S" THEN KEYED=19
410     IF KEYED$="T" THEN KEYED=20
420     IF KEYED$="U" THEN KEYED=21
430     IF KEYED$="V" THEN KEYED=22
440     IF KEYED$="W" THEN KEYED=23
450     IF KEYED$="X" THEN KEYED=24
460     IF KEYED$="Y" THEN KEYED=25
470     IF KEYED$="Z" THEN KEYED=26
480     IF KEYED$="0" THEN KEYED=27
490     IF KEYED$="1" THEN KEYED=28
500     IF KEYED$="2" THEN KEYED=29
510     IF KEYED$="3" THEN KEYED=30
520     IF KEYED$="4" THEN KEYED=31
530     IF KEYED$="5" THEN KEYED=32
540     IF KEYED$="6" THEN KEYED=33
550     IF KEYED$="7" THEN KEYED=34
560     IF KEYED$="8" THEN KEYED=35
570     IF KEYED$="9" THEN KEYED=36
580     IF ASC(KEYED$)=13 THEN LPRINT:GOTO 190
590     IF KEYED$=" " THEN LPRINT " ";:GOTO 190
600     LPRINT CYP$(KEYED);
610     GOTO 190
620     PRINT:PRINT:PRINT "Program end. One-time pad
        erased from memory."
630     CLEAR
640     END
NOW IS THE TIME FOR ALL GOOD CRYPTOS TO COME TO THE
   AID OF THEIR SYSTEMS
THIS IS A TEST
```

• • • • •

The one-time pads developed thus far in this chapter essentially are *substitution ciphers*. But this is only the

beginning. Once the operator has developed the capacity to create a string of random characters, additional work can be done to the one-time pad to further enhance basic COMSEC. The highest degree of security in one-time cryptosystem application is achieved through the use of noncarrying addition.

The Soviets generally are credited with the effective use of one-time pads that employ a series of numbers in a group format as the basis for the key.

For instance, a string of five numerical groups—45682 98713 62987 53672 71632—is the one-time pad. Characters of the alphabet are assigned a numerical value, and each group has the numerical value of each character in the message added to it. This becomes the encoded group.

The receiver of the message simply subtracts the five character group from the one-time pad group and gets the numerical value of each character. For example:

45683	98715	62980	53676	71637	CODED MESSAGE RECEIVED
-45682	98713	62987	53672	71632	ORIGINAL ONE-TIME PAD SUBTRACTION
1	2	3	4	5	OR A, B, C, D, AND E

In this application, one message character requires five encoded characters. This does enhance security; however, it obviously makes text messages 500 percent larger in bulk.

If messages must be sent quickly and securely and are short in duration, then this approach has much merit. If a message is longer and if it is a command message that must be executed immediately, this approach may be too slow. Of course, home-developed software that stores a large number of one-time pads in memory and automatically performs the arithmetic for each group, decodes the

text, and assembles or sends the same can make this approach fast, accurate, and probably the most secure system available.

Again, noncarrying addition is an important part of this approach. If the reader still is not familiar with this concept, here is an example:

```
56789   IS THE ONE-TIME PAD GROUP.
 +26    FOR THE CHARACTER "Z" IS ADDED,
        BUT THE SUM IS NOT CARRIED.

56705   IS THE ENCODED TEXT, AND WHEN ONE-TIME GROUP
56789   IS SUBTRACTED FROM THIS:

   26   THE RESULT IS NOT CARRIED OVER TO EACH
        COLUMN, AND TEXT IS DECODED.
```

The most significant drawbacks of employing the one-time pad are as follows:

1. OPERATIVE TRAINING. The entire cell must be versed in using the one-time pad without error. Storage and transportation of the pad to avoid detection and proper destruction procedures must also be stressed to each participant.

2. PHYSICAL SECURITY. Regardless of the level of training or the diligence of the operatives, unpredictable factors may allow the one-time pad to fall into the OPFOR's hands. If this occurs, it generally means that a cell member has been captured, and the other team elements may or may not be aware of it. This also means that all message traffic using the captured one-time pad that is intercepted will be decoded immediately, and anyone caught using that code will be incriminated and tied in with the person originally captured with the pad.

3. IDENTIFIABLE CHARACTERISTICS. If the OPFOR is able to intercept a number of encoded messages generated from a one-time pad, the fact that it is being employed will be established quickly by the computer

used for cryptoanalysis. As discussed earlier in this chapter, the computer is a competent codebreaker. It may not be able to break a particular code, but if it is given enough messages it can easily identify the "signature" of a one-time pad. Once this is determined, the computer can then be tasked in dissecting the message with a new set of criteria. It may or may not be successful, but the characteristics of the message will be clearly identified within a period of time.

The problem with one-time pads essentially boils down to the fact that the operative must possess a small but incriminating piece of evidence in order to protect his communications from being detected. There is, however, an alternative.

BOOK CODE

Book code is a system that employs a key to specific word locations in a common book. A book code message will contain several groups that each describe a specific page number, column, and line number in a book. For example, the code group 36819 could be decoded to mean that the word in the message is on page 368, column 1, word 9 from the top of the page. Book code is fairly secure and very easy to use. It is not as secure as a one-time pad, but the two concepts can be combined to create a means of encryption that is more secure than either approach.

Each operative is issued a copy of the same book, which will become the cell's one-time pad by using the following technique. This approach is limited to the letters of the alphabet.

By making a double-column list of all twenty-six characters as was done in creating a random one-time pad (see page 65), each operative makes his own pad as needed by using the characters in the book as the source for the random generation of characters. For instance, on

page 1 of the Bible, the first paragraph starts out with, IN THE BEGINNING GOD CREATED THE HEAVEN AND THE EARTH. The operative uses the letters of this document to create his pad. Letters are crossed off the list as they are used, and reoccurring letters in the text are passed over. For example:

```
IN THE BEGINNING GOD CREATED THE HEAVEN AND THE EARTH
AB CDE F  G          HI JK  L          M
```

As you can see from the above example, half the alphabet is already transposed using this sentence. One printed page of just about any book will contain all the letters of the alphabet except perhaps the letters Q, X, and Z. These characters can be prearranged to represent themselves. The ten numerals are not likely to be encountered in a normal book, but they can always be written out in text.

Book code is significant for two reasons. First of all, it eliminates the need to possess an incriminating one-time pad. Everyone makes his own as needed, and as long as everyone has the same book and a means of identifying the specific location used to create the pad, the security of the entire system is greatly enhanced. Also, since the random generation of the characters comes from a printed book, the trends of the code key group can not be identified by detailed computer analysis.

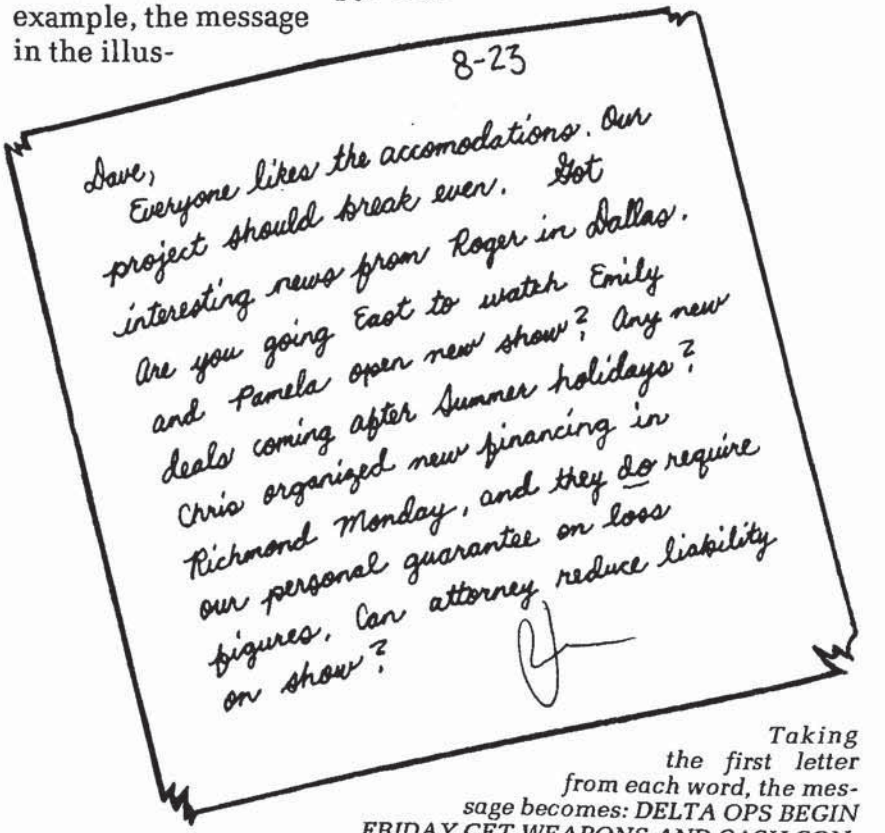
GRID CODE

As a communications planner, it is important to consider different codes and formats for each cell. In fact, it is often essential for the cell commanders to create their own method of encryption known and accessible only to the members of that specific cell. Additionally, each cell member may need to have an individual code system designed specifically for him or her.

Grid code was designed by the author to meet the

needs of a small, closely structured cell. It is simple to use and quick to teach. It has a highly random nature and is easily amenable to brevity codes and even the TAC-OPS code that will be discussed later in this chapter.

Basically, grid code inserts a message into text among many other characters. It can be as simple or as complex as needed. The basic premise of grid code is that the actual message text is at a prearranged location somewhere in the copy. For example, the message in the illus-


8-23
Dave,
Everyone likes the accomodations. Our project should break even. Got interesting news from Roger in Dallas. Are you going East to watch Emily and Pamela open new show? Any new deals coming after Summer holidays? Chris organized new financing in Richmond Monday, and they do require our personal guarantee on loss figures. Can attorney reduce liability on show?

Taking the first letter from each word, the message becomes: DELTA OPS BEGIN FRIDAY GET WEAPONS AND CASH CONFIRM AT DROP GOLF CARLOS. This handwritten note can be crumpled and "tossed" at the drop site or sent through the mail. It should look as if the recipient simply read it and threw it away. It is not very secure, but variations can be used for quick messages, backups, and as a means of communications between POWs.

tration employs a crude form of document insertion. It is not superpractical nor particularly secure—it is for example purposes only.

As you can see, the handwritten note is innocuous and seems to be fairly straightforward. In actuality, the message text is taken from the first character of each word. POWs employed this simple technique during the American Civil War. It has minimal application today except in instances where it is part of a more elaborate coding system. The basic premise, however, can be adapted.

Essentially, grid code is a somewhat complex variation of document insertion. When generated, grid code *appears* to be a random-group message of unintelligible text generated from a one-time pad. There is a high degree of random character generation in grid code, but no one-time pad is needed.

The most significant advantage of this code is that it requires no paraphernalia to either send or receive the encoded message. No tiny one-time pads to deal with, no calculator to decode numerical sequences, and no invisible ink pens or "secret decoder rings" are required. It is also user specific. A commander can send a grid code message to a specific individual, and even if others in the cell are knowledgeable about the grid code format, only the designated receiver can decode the message. There are no group identifiers or books required for this system, and it can be created and sent with one sheet of paper.

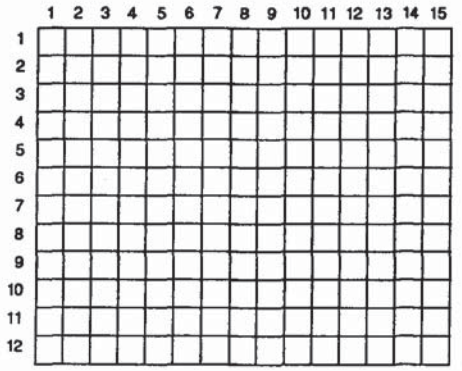
The requirements for a cell to create its own format of grid code are as follows:

1. A preset matrix or *grid* of a specific number of lines and spaces.

2. A *key-designator location* assignment for each operative and a prearranged number of characters per line or group for each key.

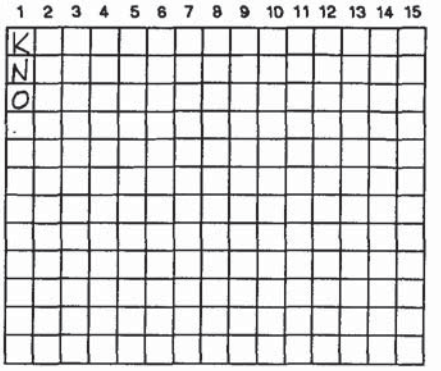
The following example is designed to walk the reader through this simple procedure.

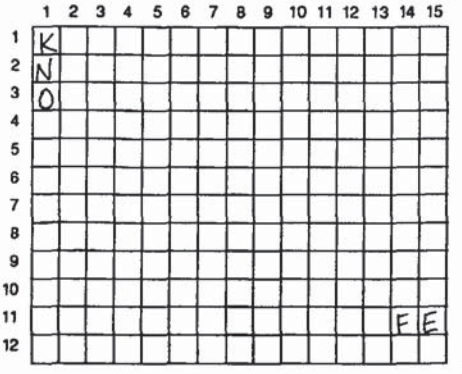
Grid code worksheet.



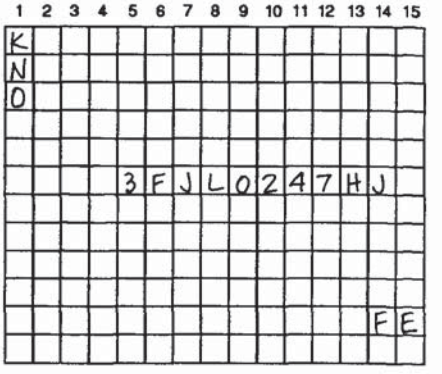
Step 1: *Create a standardized grid. A 15-character x 12-line grid is a workable size.*

Step 2: *Each operative has his own key-designator location, such as the first character in the lines 1, 2, and 3 above. This tells the receiver where the actual key designator is located in the text. KNO indicates that the key designator is on line 11, spaces 14 and 15 (K, N, and O being the eleventh, fourteenth, and fifteenth letters of the alphabet).*



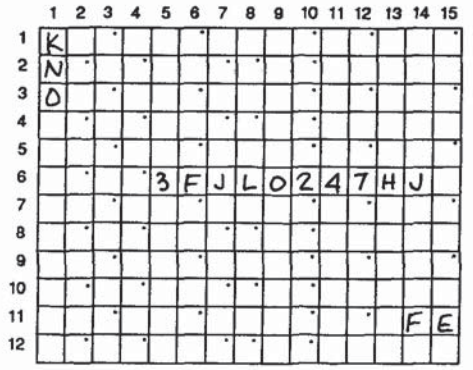


Step 3: *The key designator tells the receiver where the actual key is located in the text. FE indicates that the key begins on line 6, space 5. A prearranged set of characters (10) designating a prearranged set of characters per odd and even line (5) is entered at this location.*



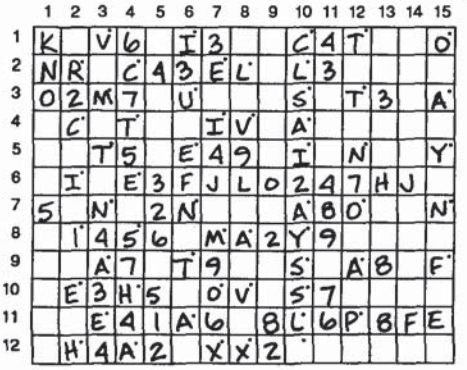
Step 4: *Actual key is placed. In this example, FE (or line 6, space 5) designates key 3FJLO247HJ, which translates to spaces 3, 6, 10, 12, and 15 on odd lines, and spaces 2, 4, 7, 8, and 10 on even lines.*

Grid code worksheet.



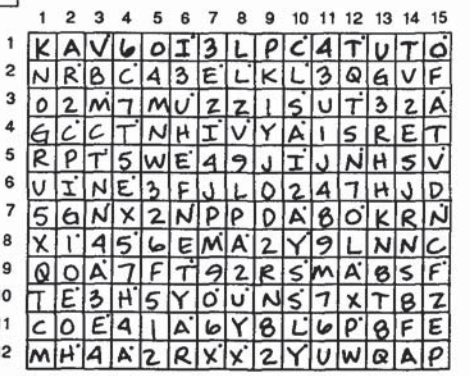
Step 5: *Mark each grid location with a dot. Note that key designators and key locations are passed over.*

Step 6: *Insert text. In this example, plain text message reads, VICTOR CELL MUST ACTIVATE IN VIENNA ON 15 MAY AT SAFEHOUSE ALPHA XX. (Note: Normally the operative would insert encoded text.)*

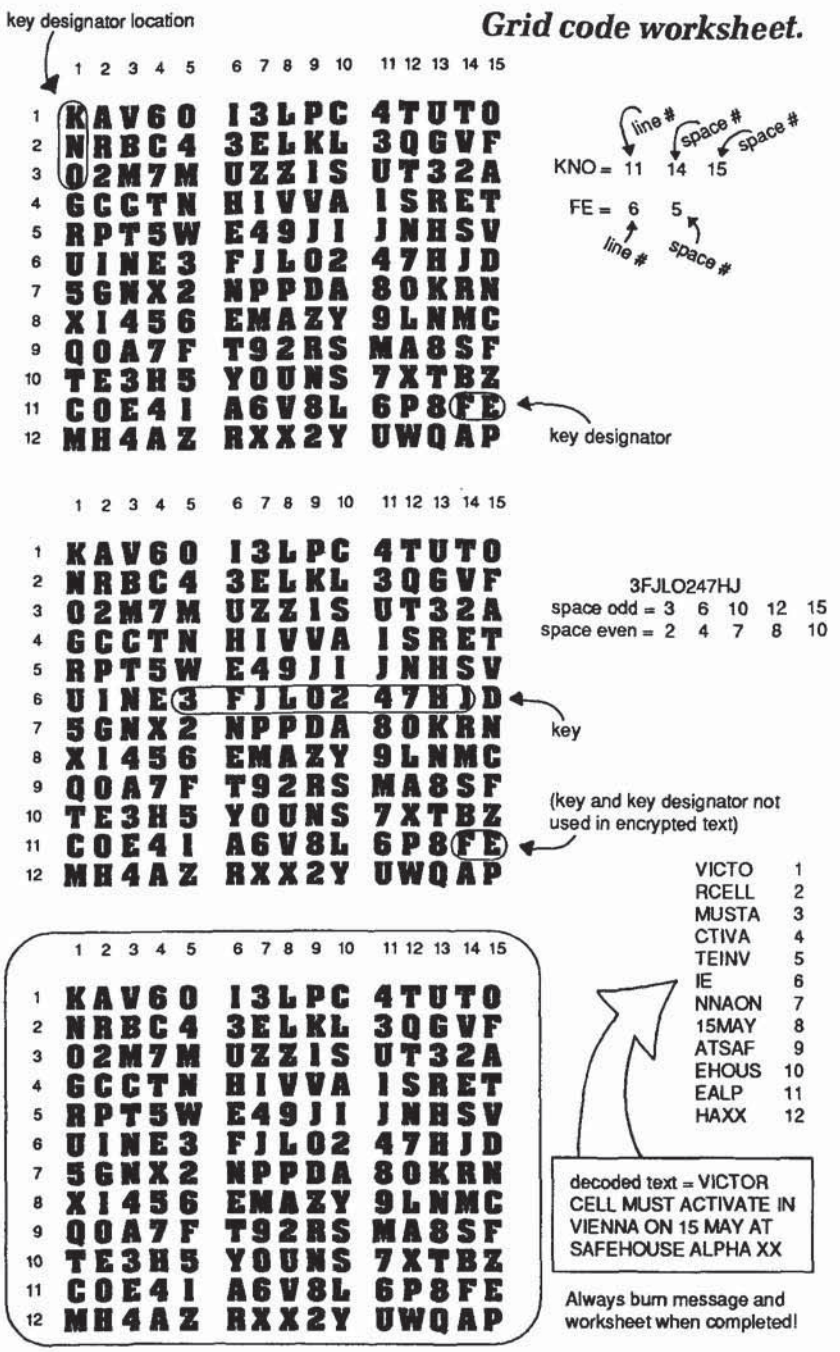
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
1 K V I C T O
2 N R C E L L
3 O M V S T A
4 C T I V A
5 T E I N V
6 I E 3 F J L O 2 4 7 H J
7 N N A O N
8 1 5 M A Y
9 A T S A F
10 E H O U S
11 E A L P F E
12 H A X X

Step 7: *After inserting text, begin to insert random numbers in empty spaces.*

Step 8: *Follow through by inserting letters randomly until the entire grid is filled. (Hint: Simply write out the alphabet while moving around the grid at random spaces until it is filled.)*

Step 9: *Rewrite the grid without the grid box and dots.*


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
1 K A V 6 O I 3 L P C 4 T U T O
2 N R B C 4 3 E L K L 3 Q G V F
3 O 2 M 7 M U Z Z 1 S U T 3 2 A
4 G C C T N H I V Y A 1 S R E T
5 R P T 5 W E 4 9 J I J N H S V
6 U I N E 3 F J L O 2 4 7 H J D
7 5 G N X 2 N P P D A B O K R N
8 X 1 4 5 6 E M A 2 Y 9 L N N C
9 Q O A 7 F T 9 2 R S M A B S F
10 T E 3 H 5 Y O U N S 7 X T B Z
11 C O E 4 1 A 6 Y B L 6 P B F E
12 M H 4 A 2 R X X 2 Y U W Q A P

Grid code worksheet.


key designator location
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
1 KAV60 I3LPC 4TUTO
2 NRBC4 3ELKL 3QGVF
3 O2M7M UZZIS UT32A
4 GCCTN HIVVA ISRET
5 RPT5W E49JI JNHSV
6 UINE3 FJLO2 47HJD
7 5GNX2 NPPDA 8OKRN
8 X145 6 EMAZY 9LNMC
9 QOA7F T92RS MA8SF
10 TE3H5 YOUNS 7XTBZ
11 COE4I A6V8L 6P8FE
12 MH4AZ RXX2Y UWQAP
line #
space #
space #
KNO = 11 14 15
FE = 6 5
line #
space #
key designator
3FJLO247HJ
space odd = 3 6 10 12 15
space even = 2 4 7 8 10
key
(key and key designator not used in encrypted text)
VICTO 1
RCELL 2
MUSTA 3
CTIVA 4
TEINV 5
IE 6
NNAON 7
15MAY 8
ATSAF 9
EHOUS 10
EALP 11
HAXX 12
decoded text = VICTOR CELL MUST ACTIVATE IN VIENNA ON 15 MAY AT SAFEHOUSE ALPHA XX
Always burn message and worksheet when completed!

Once the operative is trained in the format or size of the grid and is advised where his or her assigned key-designator location is in the text, the agent is ready to send and receive text messages without any written procedure or encryption paraphernalia. The random nature of the text—which, in the example, represents 66 percent of the encrypted message—and the intentional formatting of the text into five-character pseudogroups provide an extremely secure encryption.

As long as the operative keeps his specific key-designator location secret, his personal traffic cannot be decoded by others, even if they are familiar with the grid code concept. Plain or encrypted text can be used with grid code with a fairly high degree of COMSEC. Once the communications officer understands the basic concept of grid code, there is no way for the system to be reliably or regularly attacked by a computer or cryptoanalysis unit.

The critical security element in planning a grid code system for a decentralized underground operation is the creative placement of each agent's key-designator location. Avoid beginning or side or end of matrix key designators (it is done so in the example only for clarity). Place them in the text at different locations on vertical, horizontal, or diagonal planes on the grid matrix.

The most significant application for grid code is the potential concealment of other codes. Plain-text grid code is fairly secure; however when TAC-OPS code, one-time pad code, or book code is concealed inside of a grid code, the mathematical possibility of anyone successfully attacking the code is literally impossible to calculate.

Depending on the nature of your enterprise, effective encryption of text messages will be determined by the ability of your opposition to attack the code. The more sophisticated the opposition, the more sophisticated the code. It can be said that encryption and COMSEC procedures are designed more for the opposition than they are for the operation.

As a communications officer, you must create the most secure code possible while considering both the opposition and the level of skill among members of the cell. Training is the key. A constant assessment of the level of training, the skill of the operatives, and the quality of the code is a basic requirement for any COMMO plan.

Codes should always be simple to employ. They can be "complex in their simplicity," but they should always be user friendly in execution. Most of the procedures should be committed to the operative's memory. A variety of code plans provides you with "backups of your backups" for when things go wrong. Of course in covert ops, things *do* tend to go wrong.

TAC-OPS Code

The U.S. military employs a versatile code for routine message traffic, known as *TAC-OPS* (Tactical Operations) code. It consists of a three-character group, or *trigram*, that designates a specific word. A pocket-size dictionary of all available words for use in this format is issued to each unit. Each sixteen-page code book is normally used for one day only and then destroyed. NATO's maximum of forty-eight hours of use makes it one of the most secure and reliable military codes. It is simple to use and is an excellent example of a combination of a one-time cryptosystem and a form of book code.

TAC-OPS code (NSA designation KTC 600) has been carefully thought out for field use. There are over 1,300 trigrams for common military terms, as well as all letters and numbers. There are also a large number of *spare* locations that can be unit specific (there are 117 spare trigrams in the TAC-OPS code pictured here). Also note that commonly used letters and words have a number of available trigrams. The letter T, for instance, has six possible trigrams available to the user, and the user is advised on page 1 of the code book to use the duplicates, or *variants*, on a random basis.

TAC-OPS code.

Classroom Trng - Tactical OPS Code (P Type)
SOI Item No.

Formal authorization not required. Drop accountability on issue to user.
a. Use of plain text in conjuction with this code is prohibited. b. When placed in effect by user, this set will continue in effect for a maximum of 48 hours. c. It is essential that all variants be used impartially and at random.

GNM A	CIX Air field/port	XPI Anti	AHF Aviator/pilot
CWD A	JUD Air Force	PTE APC	EZY Axis (of)
JOZ A	HDO Air Liaison Off	DTU Apply	WAJ Azimuth (of)
SER A	RBZ Air strike	EXJ Approach-ed-s	
CRZ A 22 beg	LTG Airborne	OOJ Approach-ing	COX B
HOV Abdomen	XCB Aircraft	IFZ Approve/Aid-g	DYG B
LLA Able-ability	LTW Airdrop-s	YVI Approximat-ly	RFT Back-ed-ing
COU Abort-s ed-ing	WUK Airhead	TJS Area-s	VPE Bad
OIL Above	CRE Airmobile	GOU Area-s	CHL Barbed wire
PSH Abrasion	USM AK 47	WDD Arm-s-ed	JPR Barrage-s
ELZ Accident-al-s	UMF Al	RGZ Armor-ed	FTV Barrage-s
OXU Accomplish-ed	CHU Alert-ed-ing	IBF Army-ies	MSQ Barrier
IXZ Accomplish-ed	SPT Alive	MTM Around	SWV Base-d-s-ing
SIQ Accomplishing	BJC Alt	YNQ Arrange-d-ing	MFQ Battalion-s
PDY Acknowledge-d-ment	AAQ Alt Cdrs-rept	JPX Arrange-ment	TFR Battalion-s
	UPS Alt S3's rept	TUE Arrive-al-d-ing	EYG Battery-ies
DOG Action-ing-s	KDR Alley	GHW Artillery	WQJ Battle-s
KWR Active-ivity-s	OUK Alternate	HUG Artillery	LRB Be-aming
YZH Act as relay	VMK AltCP in comd	BYK ary	PWT Beach-ed-s-ing
ULC Add-ed-itional	UNE Alternate CP	TWC ASAP	VWY Before
YXD Add-ing-s	BSW Alt supply rt	VRY Assault	EZV Behind
LSC Adjacent	RFX Ambulance	TNE Assemble-d-ing	ACK Below
UWY Administration	ORP Ambush-ed-ng	WAZ Assist-ance	PDC Between
HCW Administrative	WBL Ambush-ed-ing	DIN Assist-ed-ing	ULZ Beyond
JBV Admit	CZZ Am-in pos (to)	RHB At (once)	UEJ Bike
TVE Advance-d-ing	VMM Ammunition	PVU Attach-ed-ing	UIO Bivouac-ed-ng
CAT Advisors	QUO Ammunition	XWO Attach-ment	NOU Black
FTG Affirmative	YIH Amphibious	XZG Attack-ed-ng-s	KCZ Bleed
VTM Age	YOE Amputate	VWL Attack-ed-ng-s	OWU Block-ed-ing-s
WHP Agent-s	BSM ance	TQW Authorization	JWH Blood
AJT Aid station-man	FUZ ANGLICO	AMD Authorize-d-ing	LMB Blow-ew own
TDM Air evacuation	KVW Answer-d-ing-s	AGG Available	XJF Blow-ing (up)

AKH Blue	CDG Challenge-d-g	JLD Concur	OTP Danger
WPK BMNT	JLS Change-d-s-ng	MIQ Condition-d-ng	BNQ Darkness
NIX Boat-s	QLF Charge-d-s	OBB Conduct-ed-ng	KLH Day-s/date-s
YFW Bomb-d-r-ng-s	QHQ Check-ed-ng-s	FKF Confidential	YQU Deadline-d-ing
XQH Bomb-d-r-ng-s	PAW Chemical-s	MKP Connect-ed-g	DPK Death
DOZ Bombardment	KDQ Chief (of Staff)	OHK Connect-ion	RAT Deception
UCK Booby trap	SXC Child	RTM Conservation	IUM Decontami-nate-d-ion
DQA Boundary-ies	QZD Civil-ian-s	LWZ Conserve-d	
LSL Breach	BZG Clarify-ication	DWG Consolidate-d	RCK Decrease-d-ng
TMS Break/broke-n	LHD Class-ify	HMQ Consolidate-ng	KXW DEFCON
XIQ Breast	RZM Classification	NJM Consolidation	YFF Defend-ed-g-s
TQK Bridge-d-ing-s	XPR Clear-ed-ance	LQX Contact-ed-s	AVS Defense-sive
WIP Brigade	FQJ Clear-ing-s	XRO Contact-ing	END Degree-s
TOX Brigade	IQQ Close-d-ing	EJU Contaminate-d	EBQ Delay-ed-ing-s
DWR Brush pile	HTM Closed in new position	EOL Contaminate-n	CQZ Delete-d-ion
BAP Build-ing-s	KMG Coast-s al	TQV Continue-d-ing	KIY Delete/omit
IPS Bulldozer	FTX Collapse	MAG Continue-ation	NLS Deliver-ed-ing
LHJ Bunker-s	LIC Collect-ed-ion	SPQ Control-d-ng-s	BFK Demolition
XUU Burst-ing-s	NWE Collect-ing-s	YNL Conversation	TNU Demonstrate-d-ing
QLP By	LZN Column-s	BWY Convoy-s	VAZ Demonstrate-d-s-ion
WQS Bypass-d-s-ng	EKN Combat	BHV Coord-s-d-ing	
	JCE Combat	XCU Coord-s-d-ing	GLD Deny-ied-ies
AZV C	WJC Come-ing	OUR COPL	UQW Depart-d-g-ure
SLT C	HMV Command-er-ed-ing-s	WVX Corps	UKT Deploy-ed-ing
JPY Cable-s		LYZ Correct-ed-ing	SXE Deploy-ment-s
MEO Caliber	IQO Command post	PIB Correct (me)	YCU Depot (supply)
VQO Call	YKW Command post	MQT Counterattack	YQU Deputy-ies
JCR Camouflage-d	WWA Commence-d-ment	DLW Counterattack-ed-ing-s	SQM Designate-d
AIS Camouflage-ng		JSM Counterpart	PAN Designation
BJQ Camp	DSV Commit-ment	IAE Cover-ed-ing	LWC DGZ
NRM Canal-s	DSZ Commit-ted-g	IWL Craft	RQV Desk
CPU Cancel-led-s	VVS Communicate-d-ions-s	XJC Crane	POI Destination
IMZ Cancel-ling-s		HPZ Critical-ty	AFU Destroy-d-ng-s
GWA Cannon	GMR Company	EDV Cross-ed-ing	NTY Destroy-d-ng-s
EWU Capable-ility	IXF Company	BJT Crossroad-s	JDX Detach-ed-s
RWF Capacity-ies	IAQ Complete-d-ng	MEY Crushed	RRT Detach-ment-s
NOC Capsule	PAO Complete-ion	QFI Culvert	BQG Determine
DQY Capture-d-ing	YQX Compound	WXE Cut-off	UIY Diesel
LBE Carry-ied-ier-s	DZA Compromise-d-ing		JLC Dig/dug (in)
HWV Casualty-ies		WAD D	BTW Direct-d-on-ng
AMS Cavalry	IQJ Concentrate-d	DXH D	BRI Disable-d-ing
FZO CBR	VPU Concentrate-d-ing-ion-s	NRC D	NSO Disapprove-d-l
VYC Cease-s-d-ing		HFM Dagger	PHI Disperse-d-g-l
BPY Center-ed-ing	WZA Concertina	NQV Damage-d-ing	
FRP CEOI			
BQA CH-47			

JBW Displace-d-ing	XYB Enemy	RVU Fall-ed-ing	PYR Front-age-ally
LGA Displacement	GOJ Enemy	KAW Fallout	GLC Front-age-ally
AEN Dispose-d-al	NCN Engineer-d-g-s	HBE Family	PPO FSCL
HFF Disregard-d-ng	TRL Enlist-ed-ing	IPR Fatal	SLN Fuel
CZO Distance-s	ADQ Enroute	USW Favor-s-ed	QNM Fused
LZV District-s	VLW Entrench-ed	HZG Favor-able-ing	NBU Future
DKK Ditch	VCK Entrench-ment	PLT FEBA	
TJE Divert-ed-sion	WEE Envelop-ed-ing	KZS Fast/foot	KVQ G
DDV Divide	OCH Equip-ed-ment	APM Female	YJM G
RNO Division-s	JOR Equip-ing-s	USC Ferry-ies-ied-g	SMZ Gallon-s
EFY Divisions	ISR er	RGB Field-s	CUG Gas-sing-sed
YNO Downed	DCW Error	YQX Fight-er-ing	BPW Gasoline
CWO Downed a/c	HSF es	UNC Fight-er-ing	UCZ Gate
BUF Drop-ping-ped	IYM Escape-d-ing	SNZ Final	NQY General-ize
IDC Drop-ping-ped	EWT Establish-d-ing	IMJ Fired-ing-s	ULG Generator(set)
TRO Due My	UVN Establish-d-ing	DJT Fixed wing	HCS Get-ting
BCX Dump-ed-ing	OML Establ-ed contact at (time)	ADS Flame-d-ing-s	GTK Give-n-ing
VOT During		EEQ Flame thrower	WDC Going (to)
	UIB Estimate-d-ing	VMP Flank-ed-ing-s	JVX Good
DNW E	BJM Estimate-ion	TAF Flank-ed-ing-s	ULR GOPL
PUO E	EKK ET	SZS Flare-d-s	IKF Grade-d-r-ing
OTL E	XZE ETA your loc	UGP Flesh	HNV Green
JMZ E	MFH ETA your loc	HRB Flash range ng	JIX Grenade-s
NZJ E	MPT ETD	CGG Fled	SBM Grid (coord)
EDU E	TNB Evacu-d-ing-ion	VMZ Flesh	XPL Grid (coord)
TON E	DLI Evacu-d-ing-ion	VXV Flexible-ility	RHT Ground-s ed
CMV East-ern (of)	SSR Execute-d-ing	BWW Flight	SRE Ground-s-ed
YAX Echelon	WJI Execute-ions-s	RPZ Follow-ed-ing-s	PZF Group
SUW ed	WKH Exhaust-ed-ing	BMQ For	WMT Guard-ed-ing-s
MXB Effect-ed-ing	RSP Expect-ed-ing	IMO Force-s-d-ing	DWQ Guerrilla-s
KNN Effective-s	RED Expect-ation-s	IUZ Fordable	BSZ Guide-d-s-ing
XXZ Element-s	UGY Expedite-d-ing	RWD Fog	VIJ Guide-ance
KJI Elevate-d-ion	TZR Explode-d-s	PJT Forearm	FZQ Guns
THI Embank-s-ed	YSJ Exploit-ed-ing	NIX Forest-s	KTV Guns
TSJ Embankment	EYU Explosive-s	KRI Fortify-ied	
EIY Emergency	JKT Expose-d-ing	MJW Fortify-ication	TKE H
FPY Emergency	YIP Extend-d-g-ive	DMS Forward-ed-ng	YBT H
YXP Emplace-d-ing	ONW Extend-sion	SFP Found	CXG H
VOD Emplace-ment	PMQ Extend-extent	HST Foxhole	RCD Had
KBI Employ-ed-ing	BIM Extract-s-d-ing	KHO Fracture	SDB Halt-ed
AJR en		LMS Frag order	FYX Halt-ed
JZC Encounter-d-g	SWF F	KVD Frequency-ies	YZP Hand
TMZ Encrypt-ed-on	TFJ F	CAP Frequency-ies	XZP Harass-ed-ing
IIZ End-ed-ing	UGQ FAC	MNC Friend-ly	EPL Harass-ment
	NHR Facility	GPP From	IRA Have/has

YIK Hawk	JEN Inches	WIS K	WYP Low-er-est
VSL Head-ed-ing	OQQ Incident-al-s	YJV K	KBH LRRP
BRR Headquarters	LQR Increase-d-g-s	LYI Keep-s-ing	XXC ly
XPM Headquarters	NDF Indigenous	LAD Killed-in-act	
GQL Heavy	VVN Indirect	NWL Kilometer-s	WCR M
AFR Hgt of burst	DHG Individual	KIO Know-n-ing	RIL M
JTV Heli-lift	WUE Infantry		DYN M
EWO Heli-pad	XPD Infantry	EMK L	CQC M-14
LQO Helicopter-s	SSS Infiltrate-d-s	BVZ L	XCV M 16
HVR Helicopter-s	VTY Infiltrate-g-on	DVT L	DKP M 60
JCW Here	MOP Inflict	KTW Laboratory-ing	TUD Machineguns
DRW High-er est	XDU Inform-d-ation	SLB Lacerate	ING Magnetic
GWO Highway-s	CLP ing	IRS Land-ed-ing	LVL Main
TEF Hill/mt/rise-s	KRD Initial-ed-ly	BTI Large	LVG Main body
AIK Hit-ting	CLO Insert-s-ed-ing	FIX Last	SXO Main supply rt
UHU Hold-er-ing	CDY Install-d-ation	AZO Lateral	YUQ Maintain-ing-s
XEF Hospital-s	TCY Instrumental	EED Launch-d-r-ing	NRR Maintain-ed
OXC Hostile	FKV Intact	PFI Launch-d-r-ing	DWK Maintenance
MCN Hour-s ly	JWB Intel (Sum)	IXK Lay/laid	HSP Make-g/made
IUG How	XDC Inland-ed-tion	KGX Lead-er-ing	WJU Male
YHP Howitzer-s	BPO Intercept-d-or	WRT Leaflet-s	CRY Maneuver-ng-s
	OKH Intercept-ion-s	SDX Leave/left	NQS Man-ned-ning
LZK I	OXF Interfere-d-ing	CAZ Leave/left	DGF Many
OAX I	ODE Interference	AJP Left (of)	XJQ Map-ped-png-s
VJW I	WWG Internal	JKM Leg	NGA March-d-s-ing
HND I	IWN Interrogate-d	SVS Level	WOP Market
FVU Identify-ed	UFC Interrogation	RHK Liaison (off)	HKT Max (range)
UTW Identification	SGK Intersection	IOW Life	DRZ Means
AMH ied	KZX Interval	HPE Light-er-ng-d-s	LVK Measure-d
CNT ies	HBH Isolate-d-ing	WXR Limit-ed-ing-s	LQU Measure-ment
XFI If	WGS Issue-d-ing-s	TBP Line-d-s (of)	UCN Mechanic-al
PWT Illuminat-d-tion	RIH Item-s	ORA Line-d-s (of)	OVZ Mechanize-d
LZN Illuminating		XKU Listen-ed-ing	BNV MEDEVAC needed
BYM Immediately	HPW J	EWC Litter-s	CVY Medical
DGD Imminent	DGV J	YUP Litter evac need at(coord)	TJM Medium
UFX Immobilize-d-ing	CJQ Jam-med-ing	VTW Little John(LJ)	LNW Meet-ing
	KDK Jam-med-ing	CYM Load-s-ed	HRF Meet (me) (at)
GOR Impact	DCZ Jeep	PUR Local-ize-d	DRN Message-s
BOS Impassable	KJR Jet-s	EUX Locate-d-ing-s	BWE Messenger
VNH Impossible	FHO Join-ed-ing	GTZ Locate-ion(of)	VCS Meter-s
EJG Improve-d-ing	EQI Joint	JAL Logistic-al-s	LKI Meter-s
OXW Improve-ment	HNU Jump ed g(off)	FSK Look (for)	KCB Mile-s
RBG In	LVW Junction-s (rd)	KYJ Loss-es/lost	IHO Mine-d (field)
LDN Inadequate		HWB Loudspeaker	
YAH Incendiary-ies			

TAC-OPS code.

FOR OFFICIAL USE ONLY

XHT Minimum
EKV Minimized
MYU Minor
KJA Minutes
MOF Misseding
HFE Missiles
MUV Missing in Act
VHO Mission
JAV Mobility
LVX Mothballed
PSG Moon
UHW Mortar
JXD Morning
UMZ Motorized
SLY Mortars
UWM Mortars
IMN Motorized
ILJ Mountainous
SCM Mounting
RQM Moving
EXI Movement
DWM Multiple
ACB My
WWT My location is
YRJ My situation is
XRF N
SHF N
NQW N
VBW N
NKH Napalm
UBI Narrow
YJQ Naval gunfire
REJ NCO
JDH Near
TPV Needing
IWR Notified
OUM Neutralize
TNY Neutralizing
JEQ New
LYE Night
KIG Nike
ISY NILO
WBH No-non neg
GTB No nonneg
YOI No fire line
JRY None
WGD North/en (of)
LRN Not
IYZ Not later than
WIB Nothing
FTB Notify/ed/es
KXT Now
BAS Nuclear
UPH Nuc Wpns Req
FVT Numbers
RQP NVA
WXO O
HTU O
IXE O
JDU O
WDH O'A(Bird Dog)
HFK O'Hi/Mohawk
KVN Objectives
GKN Observe/d
FKT Observe/ing
BEJ Observation (post)
GCD Obstacles
WPJ Occupy/ations
WVF Occupy/ing
WEP Oder
YLR Of
VVP Offensive
XDP Officers
RJI Oil
GGV On
JZR Open/ing
EPE Operate/ding
WSE Operation/s
VFS Operate/s/al
BCW Opportunity/s
EUU Or
VGS Orange
CCL Order/ed/ing
SWN Ordnance
KER Organization
GDP Organize/d
ASL Organization
MPF Origin/al/ate
KNR Other
YIS Our
VCJ Out (of)
WBA Outpost/post
TGE Over age
DLZ Overlay
WQL Overrun
YAC P
RAG P
AHR P
WAY Paddy
NJR Pajama
BZC Panels
LMQ Parachuo s
BYR Parts
MYB Party/ies
PXU Pass/ed
PWG Passable
BTY Pass age/ing
NCS Password
AXK Past
MUS Patrol/ed/ing
BIY Patrol ed/ing
BBU Pat boat/river
DNU Penetrate/d/g
YML Penetration
BEM Percent age
WDV Perimeter
ABY Period
GSD Permission
LYB Permit/ed/ing
PKR Personnel
TAJ Personnel
GPR Phase
KGL Phase line
ADH Photograph/ed/ering s
XNC Pick up
DPC Piece/d/ing s
YZZ Pipe line
NSD Place/d/ing s
RJD Plan s/ed/ing
BGB Plan s ed/ing
TNT Platoons
HKU Platoons
AYR Point s ed/ing
MWW POL
SEC Pontoon
FCL Port (harbor)
LYD Position s/en
KWS Position s ed
PDW Possible
WMQ Post s
AWQ Postpone/d/s
GMY Postponed/ing
PNV Pound s
PNO Prepare/d/ng s
GCG Prepare/d/ng s
SGY Preparation
JVN Prevent
KSJ Priest
HLJ Primary
PTL Priority
OVV Prisoners of war
VTS Prisoners of war
GHC Probable
HXD Proceed/ed/ing
WYQ Progress/ed/ing
REA Protect/d/ing
IEH Protect/d/ion
VNF Protective
HJT Provide/d/ing
OBJ Provision
RNT Province
SWO Prov Sr Adv
YAS Psywar
RXS Pursue/d/ing/uit
RNV Q
WTB Q
GDU Quartermaster
ANZ Question/ed
TLX Query/ied
MAR R
LOA R
PKQ R
WIE R
FBX Rad I radio
GLK Radar
FOR OFFICIAL USE ONLY ENCODE 5 KTC 600 A ISET 3)

FOR OFFICIAL USE ONLY

VSD Radiation
VCW Rec air strike
IYX Req air strike
FQC Require/d/ing
MBY Require/ment
DVE Rescue
GJR Reserve/d/g/s
YMK Resist/ed/ance
FQF Resist/ing
ROX Restore/s/ed
WWZ Restore s/d/ing
CTY Restoration
EHO Restriction
KWN Restrict/ive
CIV Resupply/d/s/g
ORU Resupply/d/s/g
XVA Result s/ed/ng
MKW Return ed/ing
MVE Returnee/s
WIA Ridge/d/s
OBH Rifles
PGD Right (of)
VDV Riot/s/ed
GZX River/streams
WKF Road/s
HFQ Rocket/s
ENC Round s
GEA Round/s
XFX Route/s/d/ing
DMP Ruin s/ed
PTQ S
LUE S
HPK S
KYG S
TQM Safe/ty
DJF Sampan/s
UET Schedule/d/ing
UFD Schedule/d/s
DFW Scout ed/ing/s
LSH Screen/d/ing/s
PRS Search/ed/ing/s
PVJ Second/a/ary
EJQ Secret
JEK Section/s
FOR OFFICIAL USE ONLY ENCODE 6 KTC 600 A ISET 3)

STW Sector/s
UED Secure/d/ing
ABL Security/s
CDZ Seize/d/ing
DSK Seize/ure/s
HBC Self propelled
NDJ Send/ing/sent
WSQ Separate/d/en
JWO Sequence
CZH Serial
NIJ Service/d/able
IRN Shell/s/ing/ed
YCX Shell/s/ing/ed
KDM Shoot/ing/shot
TOJ Shoot/ing/shot
YKA Short/ed
FTI Shoulder
NFQ Sight/ed/ing
RDU Sight/ed/ing
DBP Sign ed/ing
LWD Signal/ed/ing
VFY Silent/ly/ce
OFA Simulate/d/ing
BDM Site/s
DCJ Sir/SITREP
COS Slope/s/ing/d
YRZ Slow ed/ing
KID Small/er/est
ETI Smoke/d/ing/s
FRP CEOI
YYR Soldier
NUP Soon/er/est
CWP Sortie/s
WFX South/ern (of)
CXU Speak
BKI Spearhead
EPG Sporadic
GXL Spot ted (rep)
LWY Squad/s
PZA Squad/s
HJX Squadron
NXD Stand/ing (by)
XNT Start ed/ing
IGZ Start ed/ing
FPG Station ed/s
JIF Status (report)
XRG Stay ed/ing
HVK Stop ped/ping
WTY Strafe/d/ing
VJN Street
OYR Strength/en
EOF Strike/ing/s
ELY Strike/struck
URS Strong er/est
SLO Submit ed/ing
CEV Subordinate/s
FZN Successful
IGL Sunrise
DQM Sunset
YTB Superior/ity
BHC Supplement/ed/ary
EFA Supply d/s/g
EXP Supply d/s/g
PAP Support s/d/ing
WFF Surface/d/ing
KUY Surgery
JII Surround ed/g
EJC Survey ed/s
VQC Survey/ilance
BLG Suspect/ding
WNU Swallow
EKR Switch ed/ing
RQS Swollen
WUI T
TKX T
XTY T
HYS T
IWA T
TFZ T
VUM Tactic s/al
UVP Tac Opns Cen
RWC Take/ing/took
FVZ Talk
PCQ Tank/ar/s
LVA Tank/ar/s
RFW Tank destroy/ers
FOR OFFICIAL USE ONLY ENCODE 7 KTC 600 A ISET 3)

UDY Target/s
XFW Target/s
UXA Task (force)
NVB Taxi
AHB Team ed/s
KHN ted
WEM Telephone/s
BHX Temple
MHR Tentative
TQN Terminate/d/g
PVY Terrain
PQM Territory
XSI Terrorists
VQZ There
ECB These
BHY This
HQR Through
TCM Tide
QKU Time d/ing
TCM tion
WIU To (be)
GRL Today
SIJ Tomorrow
ORI Ton s/age
SKM Tonight
JPO Top Secret
XQG Total
EMG Tow ed/ing
DYC Toward
YFL Town/vil lage/s
MYW Trace r
AGM Track ed/ing
QHY Traffic
DYB Trail er d/ng/s
BCC Train ed/ing/s
ITL Transmit/ted
VHH Transmit ted
NRE Transmission
KRZ Transport ed
VHT Transport g/s
FMY Transportation
LIA Trapped
JXT Troop/s (left)
WOC Troop/s (left)
WRH Truck ed/s/ing
TTC Truck ed/s/ing
JGU Turn ed/ing
TUA U
HZL U
HAP U 1A
CWU U-6
OYB U 8
JGH UH 1B
WPC UH 1D
UDP UH 1H(Cobra)
OCY UH 19
AUR UH 34
DWF Unable
DWT Unauthorized
JSR Under/under cover
LER Understand
NSL Understood
WJY Unidentified
LHL Unit ed/s/ing
MUB Unit ed/s/ing
VUE Until (further noticed
EUW Unusual
NLO Unwarned
WZC Up
TJW US
UNB USAHAC
LFO Use d (plat rtl
IDK V
OBF V
OMT VC (Viet Cong)
RVF Vehicle/s
SUN Vehicle/s
ASD Verify/ied
NCE Verify/ication
MCC Vertical
LSB Very
AGP Vicinity (of)
LJW Violate s/d/ing
MCY Violet
FDQ Visible/ility
CPO Vulnerable
JEZ W
VTJ W
WAB Wagon
CFH Wait ed/ing
JKW War
KFF Warehouse
ECS Warhead
PWF Warn ed/ing/s
FYA Was/were
YTS Water
PNT We/us
FHC Weak en/ness
OZC Weapon/s
GCJ Weapon/s
IFU Weather
JVJ Week/s
LLX West ern (of)
NIP What
CZT Wheel ed
FGS When
PZW Where
IAT Which
LBY White
IMU White phosphorus
NWQ Who
ATS WIA
SYJ Will
MDD Wind
HNP Wire s/d/ing
EMI With
OPN Withdraw n al
MND Withdraw ng/s
RPA Wood/s/ed
SRH Work s ed/ing
UTT Wound ed/s
GQS Wreck ed/s
ISD Wrist
PNX Wrong
GNR X
GSB X
DGO Y
KQM Y
SAM Yards
PEZ Yards
MUT Yellow
GBX Yes
DEQ Yesterday
DIY You r
YZW Z
JNM Z
PTT Zone s ing (of)
ETX 1
IMF 1
YHQ 1
FUM 1
BFL 2
PJE 2
VEJ 2
CTO 2
FMC 3
PYA 3
ICY 3
BJE 4
LAG 4
JWM 4
PXH 5
COV 5
SAJ 5
IVH 5
RBE 6
PYD 6
PRX 6
HWK 7
MKV 7
NIN 7
CZL 8
OFZ 8
OXL 8
AKY 9
EVP 9
WJL 9
FOR OFFICIAL USE ONLY ENCODE 7 KTC 600 A ISET 3)

FOR OFFICIAL USE ONLY

EFD @
NYP @
BMT @
UNT @
NSW @
ULK @
BFH @@
UTQ @@
RFP @@
WXK @@
IAB @@
BMU @@@
UHP @@@
XMK @@@
YDZ @@@
VEB 1/4
NVZ 1/2
NOT 3/4
DZD 2 1/2
YJP 30 cal
GDV 45 cal
HGT 50 cal
BSV 2.75 mm
VNB 4.2 mm
GMS 7.62 mm
FSJ 81 mm
MLT 90 mm
EWG 105 mm
PLW 106 mm
STD 155 mm
CON 3.5 inch
CJP 8 inch
MCG I (First)
IOV II (Second)
BMD III (Third)
UJK IV (Fourth)
YJO V (Fifth)
STK VI (Sixth)
TLZ VII (Seventh)
PEN VIII (Eighth)
LMD IX (Ninth)
OQU X (Tenth)
WVM Comma (,)
AFB Comma (,)
FOG Comma (,)
IZA Comma (,)
VJH Hyphen (-)
TFA Hyphen (-)
VRZ Hyphen (-)
UFP Hyphen (-)
WWF Period (.)
PUP Period (.)
SNR Period (.)
WDP Period (.)
SLJ Slant (/)
CRL Slant (/)
DDN Slant (/)
OZU Slant (/)
KFQ Spare 1
PEV Spare 2
WBQ Spare 3
KQT Spare 4
OJS Spare 5
YZQ Spare 6
QJB Spare 7
DRD Spare 8
XML Spare 9
CEF Spare 10
XDH Spare 11
JQQ Spare 12
UQZ Spare 13
WOX Spare 14
LPE Spare 15
PRJ Spare 16
PAQ Spare 17
RMV Spare 18
JQR Spare 19
UWY Spare 20
RCP Spare 21
JGA Spare 22
PBH Spare 23
THU Spare 24
XWD Spare 25
TMM Spare 26
ASW Spare 27
OKE Spare 28
KRH Spare 29
SGP Spare 30
ERY Spare 31
LAI Spare 32
OHZ Spare 33
CIC Spare 34
CSV Spare 35
WSR Spare 36
VCD Spare 37
OUQ Spare 38
MSK Spare 39
ROZ Spare 40
NWN Spare 41
DEL Spare 42
JAM Spare 43
BUW Spare 44
BBV Spare 45
ONF Spare 46
AJZ Spare 47
VDP Spare 48
UDC Spare 49
DKR Spare 50
PTZ Spare 51
OYO Spare 52
DTY Spare 53
RUD Spare 54
FOL Spare 55
URX Spare 56
SYN Spare 57
KKG Spare 58
YZN Spare 59
WBZ Spare 60
BBP Spare 61
NCJ Spare 62
TZZ Spare 63
GTO Spare 64
KUZ Spare 65
URT Spare 66
DFL Spare 67
ATW Spare 68
JBA Spare 69
CLA Spare 70
WUF Spare 71
IQK Spare 72
KPC Spare 73
BRS Spare 74
PGO Spare 75
PVK Spare 76
QOY Spare 77
SLV Spare 78
VPY Spare 79
DGS Spare 80
WFC Spare 81
HNY Spare 82
XVJ Spare 83
YAG Spare 84
EYQ Spare 85
JYW Spare 86
MHT Spare 87
XXO Spare 88
JUM Spare 89
XLO Spare 90
PZQ Spare 91
AXR Spare 92
OEB Spare 93
SJH Spare 94
AHU Spare 95
DZM Spare 96
SRA Spare 97
YXO Spare 98
LUK Spare 99
OJC Spare 100
OGR Spare 101
LRC Spare 102
DXK Spare 103
RKH Spare 104
PNI Spare 105
UHT Spare 106
AQL Spare 107
YCA Spare 108
GJO Spare 109
KUQ Spare 110
SAB Spare 111
USK Spare 112
VJP Spare 113
YES Spare 114
XZS Spare 115
XLS Spare 116
FOR OFFICIAL USE ONLY ENCODE 8 KTC 600 A ISET 3)

TAC-OPS code.

FOR OFFICIAL USE ONLY

A
AAO All Cdrs rept
ABL Secure-ity-s
ABY Period
ACB My
ACK Below
ADH Photograph-ed-er-ing-s
ADQ Enroute
ADS Flame-d-ing-s
AEN Dispose-d at
AFB Comma (,)
AFR Rgt of burst
AFU Destroy-d-ing-s
AGG Available
AGM Track ed-ing
AGP Vicinity (of)
AHB Team ed s
AHF Aviator/pilot
AHR P
AHU Spare 95
AIK Hit-ting
AIS Camouflage-ng
AJP Left (of)
AJR an
AJT Aid (sta/man)
AJZ Spare 47
AKH Blue
AKY 9
AMD Authorize-d-ng
AMH ed
AMS Cavalry
ANZ Question ed
APM Female
AQL Spare 198
ARG Reach-ed s ng
ARM Rate
ASD Verify-ied
ASL Orient-g-ation
ASW Spare 27
ATF Relay ed-ing
ATS WIA
ATW Spare 68
AUR UH 34
AVS Defense-sive

AWQ Postpone-d s
AXK Past
AXR Spare 92
AYR Point s ed-ing
AZO Lateral
AZV C

B
BAP Build-r-ng-s
BAS Nuclear
BBP Spare 61
BBU Pat boat river
BBV Spare 45
BCC Train-ed-ing s
BCW Opportunity s
BCX Dump ed-ing
BDM Site s
BDY Range
BEJ Observation (post)
BEM Percent-age
BFK Demolition
BFL 2
BFM 88
BGA CH 47
BGB Plan s ed-ing
BGG Determine
BHC Supplement ed ary
BHV Coord s d-ing

C
BHX Temple
BHY This
BIM Extract s d-ing
BIY Patrol ed-ing s
BJC Air
BJE 4
BJM Estimate-ion
BKI Spear-head
BLG Suspect d-ng
BMD III (Third)
BMQ For
BMT 8
BMU 000
BNQ Darkness

BNV MEDEVAC needed
BOA Rather
BOS Impassable
BPO Intercept d or
BPW Gasoline
BPY Center-ed-ing
BQM Move d-ing
BRI Disable d-ing
BRR Headquarters
BRS Spare 74
BSM ance
BSV 2.75 mm
BSW Alt supply rt
BSZ Guide d s ing
BTI Large
BTW Direct d on ng
BTY Pass age-ing
BUF Drop-ping-ped
BUW Spare 44
BVZ I
BWE Messenger
BWW Flight
BYK ary
BYM Immediately
BYR Part s
BZC Panel s
BZG Clarify-ication

CAP Frequency-ies
CAT Advisor-s
CAZ Leave/left
CBN Red
CCL Order ed-ing s
CDG Challenge-d-g
CDY Install d-ation
CDZ Seize d-ing
CEF Spare 10
CEV Subordinate s
CFH Wait ed-ing
CGG Fled
CGZ Delete d-ion
CHL Barbed wire
CHU Alert ed-ing

CIC Spare 34
CIV Resupply d-s-g
CIX Air (fld/port)
CJP 8 inch
CJQ Jam med-ing
CLA Spare 78
CLO Insert s ed-ing
CLP ing
CMV East-ern (of)
CNT ies
CON 3.5 inch
COS Slope s ing d
COU Abort s ed-ing
COV 5
COX 8
CPD Vulnerable
CPU Cancel led s
CQC M-14
CRE Automobile
CRL Slant (/)
CRY Maneuver-ng s
CRZ A 22 bag
CSV Spare 35
CTQ 2
CTY Restoration
CUG Gas sing sed
CVY Medical
CWD A
CWO Downed acft
CWP Sorties
CWU U 6
CXG H
CXU Speak
CYM Load s ed
CZH Serial
CZL 8
CZO Distance s
CZT Wheel-ed
CZZ Am-in pos (to)

D
DAR Replace-d-ing
DBP Sign-ed-ing
DCJ Sit/SITREP
DCW Error

DVE Rescue
DVT L
DWF Unable
DWG Consolidate-d
DWK Maintenance
DWQ Guerrilla-s
DWR Brush pile
DWT Unauthorized
DXH D
DXK Spare 184
DYB Trail-er-d-ng-s
DYC Toward
DYG 8
DYN M
DYR Strength-en
DZA Compromise-d-ing
DZD 2 1/2
DZM Spare 96

E
EBG Delay-ed-ing s
EBS Recognize-d-g
ECB These
ECS Warhead
EDU E
EDV Cross-ed-ing
EED Launch-d-ing
EEG Flame thrower
EFA Supply-d-s-g
EFD 9
EFU Repeat-ed-ing
EFY Division-s
EHO Restrict-ion
EIY Emergency
EJC Survey-ed-s
EJG Improve-d-ing
EJO Secret
EJU Contaminate-d
EKK ET
EKN Combat
EKR Switch-ed-ing
EKV Minimize-d
ELY Strike/struck
ELZ Accident-al-s

EMG Tow-ed-ing
EMI With
EMK L
ENC Round-s
END Degree-s
EOF Strike-ing-s
EOL Contaminate-n
EPE Operate-d-ing
EPQ Sporadic
EPL Harass-ment
EQI Joint
ERY Spare 31
ETJ Smoke-d-ing-s
ETX 1
EUU Or
EUW Unusual
EUX Locate-d-ing-s
EVP 9
EWC Litter-s
EWD 106 mm
EWO Halo pad
EWT Establish-d-ng
EWU Capable-ity
EXI Move-ment
EXJ Approach-ed-s
EXP Supply-d-s-g
EYG Battery-ies
EYQ Spare 85
EYU Explosive-s
EZB Remain-ed-der

EZV Behind
EZY Axis (of)

F
FBX Rad (rad/hr)
FCL Port (harbor)
FDQ Visible-ility
FGJ Clear-ing-s
FGS When
FHC Weak-en-ness
FHO Join-ed-ing
FIX Last
FKF Confidential
FKQ Repulse-d-ing
FKT Observe-s-ing

FKV Intact
FKX Reinf-ment-s
FMC 3
FMY Transportation
FOG Comma (,)
FOL Spare 58
FPG Station-ed-s
FPY Emergency
FQC Require-d-ing
FQF Resist-ing
FRP CEOI
FSJ 81 mm
FSK Look (for)
FTB Notify-ied-ies
FTG Affirmative
FTI Shoulder
FTV Barrage-s
FTX Collapse
FUM 1
FUZ ANGLICO
FVC Number-s
FVU Identify-ed
FVZ Talk
FYA Was/were
FYX Halt-ed
FZN Successful
FZO CBR
FZQ Gun-s

G
GBX Yes
GCD Obstacle-s
GCG Prepare-d-ng-s
GCJ Weapon-s
GDP Organize-d
GDU Quartermaster
GDV 45 cal
GEA Round-s
GFI Culvert
GQL Heavy
GQV On
GMQ Probable
GHQ Check-ed-ng-s
GHW Artillery
GJQ Spare 118

FOR OFFICIAL USE ONLY
DECODE 1 KTC 600 A (SET 3)

FOR OFFICIAL USE ONLY
DECODE 2 KTC 600 A (SET 3)

FOR OFFICIAL USE ONLY

GJR Reserve-d-g-s
GKN Observe-d-r
GLC Front-age-ally
GLD Deny-ied-ies
GLF Charge-d-s
GLK Radar
GLP By
GMR Company
GMS 7.62 mm
GNY Postpone-ing
GNM A
GNR x
GOJ Enemy
GQR Impact
GOU Area s
GPP From
GPR Phase
GQS Wreck-er-ed s
GRL Today
GSB x
GSD Permission
GTB No/non-neg
GTD Spare 64
GTK Give n-ing
GTZ Locate-n/o(f)
GUR COPL
GWA Cannon
GWO Highway s
GXL Spot-ted (rept)
GZD Civil-ian-s
GZX River stream s

H
HAP U-1A
HBC Self-propelled
HBE Family
HBM Isolate-d-ing
HCS Get-ting
HCW Administrative
HDO Air Liaison Off
HFE Missile s
HFF Disregard-d-ng
HFK OV1/Mohawk
HFM Dagger
HFQ Rocket s

HGT 50 cal
HGV Damage d-ing
HHQ Consolidate-ng
HJT Provide d-ing
HJX Squadron
HKT Max (range)
HKU Platoon s
HLJ Primary
HMK 7
HMV Command er ed-ing s
HND I
HNP Wire-s d-ing
HNU Jump-ed (off)
HNV Green
HNY Spare 82
HOV Abdomen
HPE Light-er-ng d-s
HPK S
HPW J
HPZ Critically
HQR Through
HRB Flash-range-ng
HRF Meet (me) (at)
HSF es
HSP Make g-made
HST Fuel/oil
HTM Closed in new position
HTU O
HUG Artillery
HVK Stop ped-ping
HVR Helicopter s
HWB Loudspeaker
HWV Casualty-ies
HXD Proceed ed-ng
HYS T
HZG Favor able-ing
HZL U

I
IAB 88
IAE Cover ed-ing
IAQ Complete d-ing
IAT Which

IBF Army-ies
ICY 3
IDC Drop-ping-ped
IDK V
IEH Protect d-ion
IFU Weather
IFZ Approver al-3-g
IGG Close d-ing
IGJ Concentrate-d
IGL Sunrise
IGZ Start ed-ing
IHF 1
IHQ Mine-d (field)
IIZ End ed-ing
IKF Grade d-r-ing
IKZ Raid-er-ing-s
ILJ Mountain-ous
IMJ Fire d-ing-s
IMN Motor-ized
IMO Force-s d-ing
IMU White phosphorus
IMZ Cancel ling-s
ING Magnetic
INT Platoon s
IOV II (Seconds)
IOW Life
IPR Fatal
IPS Bulldozer
IQD Command post
IQK Spare 72
IRA Have/has
IRN Shell s-ing ed
IRS Land ed-ing
ISD Wrist
ISR in
ISY NILO
ITL Transmit ted
IUG How
IUH Decontamin-nate d-ion
IUZ Ford able
IVH S
IVN Prevent
IVX Monk/bonze

IWA T
IWL Craft
IWN Interrogate d
IWR Net ted-ting
IXE O
IXF Company
IXK Lay/laid
IXZ Accomplish-ed
IYM Escape d-ing
IYR Spare 182
IYX Req air strike
IYZ Not later than
IZA Comma (,)
IZN Illuminat-ing

J
JAL Logistic-al-s
JAM Spare 43
JAV Mobile-ity
JBA Spare 69
JBV Admin
JBW Disable d-ing
JCE Combat
JCR Camouflage d
JCW Here
JDH Near
JDU O
JDX Detain ed-s
JEK Section s
JEN Inch es
JEO New
JEZ W
JGA Spare 22
JGH UH-1B
JGU Turn ed-ing
JIF Status (report)
JIJ Surround ed-g
JIX Grenade s
JKM Leg
JKT Expose d-ing
JKW War
JLC Dig/dug (in)
JLD Concur
JLS Change d-s-ng
JMZ E

FOR OFFICIAL USE ONLY
DECODE 3 KTC 600 A (SET 3)

FOR OFFICIAL USE ONLY

JNM Z
JOM Recover ed-y
JOR Equip-ing s
JOZ A
JPO Top Secret
JPR Barrage-s
JPX Arrange-ment
JPY Cable s
JQC Spare 188
JQO Spare 12
JQR Spare 19
JRY None
JSW Counterpart
JSR Under/under cover
JTV Helo-lift
JUD Air Force
JUM Spare 89
JVJ Week s
JVX Good
JWB Intel (Sum)
JWH Blood
JWW 4
JWO Sequence
JXD Morning
JXT Troop s (lift)
JYW Spare 86
JZC Encounter d-g
JZR Open ed-ing

K
KAW Fallout
KBH LRRP
KBI Employ ed-ing
KCB Mile-s
KCZ Bleed
KDK Jam-med-ing
KDM Shoot-ing/shot
KDQ Chief (of Staff)
KDR Alley
KER Organize-ation
KFF Warehouse
KFQ Spare 1
KGL Phase line
KGX Lead-er-ing

KHN ted
KHO Fracture
KID Small-er est
KIG Nike
KIO Know-n-ing
KIY Delete/omit
KJA Minute s
KJI Elevate-d-ion
KJR Jet s
KKG Spare 58
KLH Day s/date s
KMG Coast s al
KNN Effect-ive s
KNR Other
KPC Spare 73
KPH Radiological
KQM Y
KQT Spare 4
KRD Initial ed ly
KRH Spare 29
KRI Fortify-ied
KRZ Transport ed
KSJ Priest
KTV Gun s
KTW Labor ed-ing
KUQ Spare 111
KUY Surgery
KUZ Spare 65
KVD Frequency-ies
KVN Objective s
KVQ G
KVW Answer d-ng-s
KWN Restrict-ive
KWR Act-ive-ivity s
KWS Position s ed
KXT Now
KXW DEFCON
KYG S
KYJ Loss es/lost
KZS Feet/foot
KZX Interval

L
LAD Killed in act
LAG 4

LAI Spare 32
LBE Carry-ied on s
LBY White
LDN Shelter-ate
LER Understand
LFQ Use d glair-rt
LFS Recoilless rifl
LGA Displace-ment
LHB Blow ew-own
LHD Class-ify
LHJ Bunker s
LHL Unit ed-s-ing
LIA Trapped
LIC Collect ed-ion
LIH Repel-ed-ing s
LJW Violate-s d-ing
LKI Meter-s
LLA Able/ability
LLX West-ern (of)
LMD IX (Ninth)
LMQ Paratroop-s
LNS Frag order
LNW Meet-ing
LOA R
LPD Railhead
LPE Spare 15
LQO Helicopter-s
LQR Increase d-g-s
LQU Measure ment
LQX Contact ed-s
LRB Be en ing
LRC Spare 183
LRN Not
LSB Very
LSG Adjacent
LSH Screen d-ng-s
LSL Breach
LTC Rear
LTG Airborne
LTN Reference (to)
LTW Airdrop s
LUE S
LUK Spare 99
LVA Tank-er-s
LVG Main body

LVK Measure-d
LVL Main
LVW Junction-s (rd)
LWC OGZ
LWD Signal-ed-ing
LWY Squad s
LWZ Conserve d
LYB Permit-ed-ing
LYD Position-s-ed
LYE Night-s
LYI Keep s-ing
LYZ Correct-ed-ing
LZK I
LZN Column-s
LZV District-s

M
MAG Continue-ation
MAH Reinf-ed-s-ing
MAR R
MBY Require-ment
MCC Vertical
MCG I (First)
MCN Hour-s-ly
MCY Violet
MDD Wind
MEQ Caliber
MFC Spare 81
MFF Surface d-ng
MFH ETA your loc
MFQ Battalion-s
MFX South-ern (of)
MGT Counterattack
MHR Tentative
MHT Spare 87
MIQ Condition-d-ng
MIX Boat-s
MJL 9
MJQ Camp
MJT Cross/road-s
MJU Male
MJW Fortify-ication
MKP Connect-ed-g
MKV 7
MKW Return-ed-ing

FOR OFFICIAL USE ONLY
DECODE 4 KTC 600 A (SET 3)

TAC-OPS code.

FOR OFFICIAL USE ONLY

MLT 90 mm
MMS Registrat'n pl
MMW POL
MNC Friend ly
MNO Withdraw ng s
MQP Inflict
MPF Origin al ate
MPT ETD
MQJ Battle s
MSK Spare 39
MSQ Disapprove d
MSQ Barrier
MTJ Regiment s
MTM Around
MTY Strafe d ing
MUB Unit ed s ing
MUE Infantry
MUI T
MUS Patrol ed ing s
MUT Yellow
MUV Missing in act
MVE Returnee s
MVM Comma ( )
MWF Period ( )
MWT My location is
MWY Convoy s
MXB Effect-ed ing
MXK 00
MYB Party ies
MYP 0
MYU Minor
MYW Trace r

N

NBU Future
NCE Verify ication
NCJ Spare 62
NCN Engineer d g s
NCS Password
NDF Indigenous
NDJ Send ing/sent
NEY Crushed
NFO Sight ed ing
NGA March d s ing
NHG Recon
NHR Facility
NIJ Service d able
NIN 7
NIP What
NIX Forest s
NJM Consolidation
NJR Pajama
NKH Napalm
NLO Unwarned
NLS Deliver ed ing
NOC Capsule
NOT 3/4
NQU Black
NQS Man-ned ning
NQW N
NQY General ize
NRC D
NRE Transmission
NRM Canal s
NRR Maintain ed
NSD Place d ing s
NSL Understood
NSW 0
NTH Relief/relieve
NTY Destroy d ing s
NUP Soon er est
NVB Taxi
NVZ 1/2
NWE Collect ing s
NWL Kilometer s
NWN Spare 41
NWQ Who
NXD Stand ing (by)
NZJ E

O

OAX I
OBB Conduct ed ng
OBF V
OBH Rifle s
OBJ Provide sion
OCH Equip ed ment
OCY UH 19
ODE Interfere nce
ODR Release d ng s
OEB Spare 93
OEK Regroup ed ng
OFA Simulate d ing
OFB Repair ed ing
OFZ 8
OGR Spare 101
OHK Connect ion
OHY Traffic
OMZ Spare 33
OIL Above
OJB Spare 7
OJS Spare 5
OKE Spare 28
OKH Intercept ion s
OKU Time d ing
OML Estab ed con tact at (time)
OMT VC (Viet Cong)
ONF Spare 46
ONM Fuse d
ONW Extend sion
OOJ Approach ing
OOY Spare 77
OPN Withdrawn n al
OQQ Incident al s
OQU X (Tenth)
ORA Line d s (of)
ORI Ton s ege
ORP Ambush ed ng
ORU Resupply d s g
OTA Report ed ing
OTL E
OTM Reference d s
OTP Danger
OUK Alternate
OUM Neutral ize
OUO Ammunition
OUQ Spare 38
OVV Pris s of war
OVZ Mechanize d
OWU Block ed ing s
OXC Hostile
OXF Interfere d ing
OXL 8
OXU Accomplish ed
OXW Improve ment
OYD Spare 52
OYW U-8
OZC Weapon s
OZU Slant (/)

P

PAD Spare 17
PAN Designate ion
PAO Complete ion
PAP Support s-d ng
PAW Chemical s
PBH Spare 23
PCQ Tank er s
PDC Between
PDY Acknowledge d-ment
PEN VIII (Eighth)
PEV Spare 2
PEZ Yards
PFI Launch-d ring
PGD Right (of)
PGO Spare 75
PHI Dissipate d g i
PIB Correct (me)
PII FEBA
PJE 2
PJT Forearm
PKQ A
PKR Personnel
PLW 106 mm
PMQ Extend-extent
PMT Beach-ed s ng
PNI Spare 106
PNO Prepare d ng s
PNT Wa/us
PNV Pound s
PNX Wrong
POI Destination
POW Possible
PPO FSCL
PQM Territory
PRJ Spare 16
PRS Search d ng s
PRX 6

FOR OFFICIAL USE ONLY DECODE 5 KTC 600 A ISET 3

FOR OFFICIAL USE ONLY

PSG Moon
PSH Abrasion
PTE APC
PTL Priority
PTQ S
PTT Zone-s ing (of)
PTZ Spare 51
PUQ E
PUP Period ( )
PUR Local-ize-d
PVJ Second-s-ary
PVK Spare 78
PVU Attach ed-ing
PVY Terrain
PWF Warn-ed-ing-s
PWQ Pass-able
PWT Illuminat-d-ion
PXH 5
PXU Pass es-ed
PYA 3
PYD 8
PYR Front-age-ally
PZA Squad s
PZF Group
PZM Where
PZQ Spare 91

R

RAQ P
RAN Reduce-g-tion
RAT Deception
RBE B
RBG In
RBZ Air strike
RCD Had
RCK Decrease-d ng
RCP Spare 21
RDU Sight-ed-ing
REA Protect-d-s ng
RED Expect-ation s
REJ NCO
RFM Tank destroy er s
RFP 00
RFT Back-ed-ing

RFX Ambulance
RQB Field-s
RQZ Armor ed
RHB At (once)
RHK Liaison (off)
RHT Ground-s-ed
RIH Item-s
RIL M
RJD Plan-s-ed-ing
RJI Oil
RMF Capacity-ies
RMV Spare 18
RND Division-s
RNT Province
RHV Q
ROX Restore-s-d
ROZ Spare 40
RPA Wood-s-ed
RPZ Follow-ed-ng-s
RQP NVA
RQS Swollen
RQV Dask
RRH Spare 105
RRT Detach-ment-s
RSP Expect-ed-ing
RTM Conservation
RUY Recon
RVU Fail-ed-ing
RVW Vehicle-s
RWC Take-ing/took
RWD Fog
RXS Pursue-d-ing-it
RZM Classification

S

SAB Spare 112
SAJ S
SAM Yards
SBM Grid (coord)
SCM Mount-ed-ing
SDB Halt-ed
SDX Leave/left
SEC Pontoon
SER A
SFP Found

SGK Intersection
SGP Spare 30
SGY Preparation
SHF N
SIJ Tomorrow
SIQ Accomplishing
SJH Spare 94
SKM Tonight
SLB Lacerate
SLJ Slant (/)
SLN Fuel
SLO Submit-ed-ing
SLT C
SLV Spare 78
SLY Mortar-s
SMB Radio-s
SMO Prov Sr Adv
SMZ Gallon-s
SNR Period ( )
SNZ Final
SPG Control-d-ng-s
SPT Alive
SQM Designate-d
SRA Spare 97
SRE Ground-s-ed
SRH Work-s-ed-ing
SSR Execute-d-ing
SSS Infiltrate-d-r-s
STD 155 mm
STK VI (Sixth)
STW Sector s
SUN Vehicle s
SUW ed
SVS Level
SWF F
SWN Ordnance
SWV Based-s ing
SXC Child
SXE Deploy ment-s
SXQ Main supply rt
SYD Ready
SYJ Will
SYN Spare 57
SZS Flare d s

T

TAF Flank-ed-ing s
TAJ Personnel
TBP Line d s (of)
TCM tion
TCW Tide
TCY Instrumental
TDM Air evacuation
TEF Hill/mt/rise-s
TFA Hyphen (-)
TFJ F
TFR Battalion-s
TFZ T
TGE Over-age
TQV Continue-d-ing
TQX Compound
TMI Embank-s-ed
TMU Spare 24
TMZ Encrypt-ed-ion
TJE Divert ed-sion
TJM Medium
TJS Area/s
TJW US
TKE H
TKX T
TLX Query-ied
TLZ VII (Seventh)
TNM Spare 26
TNS Break/broke-n
TNY Neutralize-d-g
TNB Evac-d-ing-ion
TNE Assemble-d-ng
TNU Demonstrate-d ing
TQJ Shoot-ing/shot
TQK Bridge-d-ing-s
TQN E
TQW Authorization
TQX Brigade
TPV Need-ed-ing
TQM Safe-rity
TQN Terminate-d g
TRL Enlist-ed ing
TRQ Due My
TSJ Embank ment

FOR OFFICIAL USE ONLY DECODE 6 KTC 600 A ISET 3

FOR OFFICIAL USE ONLY

TTC Truck-ed s ing
TUA U
TUD Machinegun s
TUE Arrive al-d ing
TVE Advance d-ing
TWC ASAP
TYN Receive r d-ng
TZR Explode d s
TZZ Spare 83

U

UBI Narrow
UCK Booby trap
UCN Mechanic al
UCZ Gate
UDC Spare 49
UDP UH-1H(Cobra)
UDY Target-s
UEO Secure-d ing
UEJ Bike
UET Schedule d-ing
UFC Interrogate-ion
UFD Schedule d s
UFP Hyphen ( )
UFX Immobile-ize d ing
UGP Flash
UGQ FAC
UGY Expedite d-ing
UHP 000
UHT Spare 107
UHU Hold-er ing
UHW Morale
UIB Estimate d-ing
UIO Bivouac ed ng
UIY Diesel
UJK IV (Fourth)
UKT Deploy-ed ing
ULC Add-ed-itional
ULG Generator(set)
ULK 9
ULR GOPL
ULZ Beyond
UMF at
UMZ More/most
UNB USAHAC
UNC Fight-er ing
UNE Alternate CP
UNT 0
UPB Nuc Wpns Req
UPS All S3's rept
UQJ Ration-s ed
UQW Depart-d g ure
UQZ Spare 13
URS Strong-er est
URT Spare 66
URX Spare 56
USC Ferry ies red g
USK Spare 113
USM AK 47
USW Favor s ed
UTQ 00
UTT Wound-ed s
UTW Identification
UVN Establish-d-ng
UVP Tac Ops Cen
UWM Mortar s
UWR Report s (to)
UWV Administration
UWY Spare 20
UXA Task (force)

V

VAZ Demonstrate d-sion
VBW N
VCD Spare 37
VCJ Out (of)
VCK Entrench ment
VCS Meter s
VCW Req air strike
VDP Spare 48
VDV Riot s ed
VEB 1/4
VEJ 2
VFS Operate s al
VFY Silent ly ce
VGI Range
VGO Call
VGS Orange
VHD Mission s
VHH Transmit-ted
VHT Transport g s
VIJ Guide ance
VJH Hyphen ( )
VJN Street
VJP Spare 114
VJW 1
VLW Entrench ed
VMB 4.2 mm
VMK AltCP in comd
VMM Ammunition
VMP Flank-ed-ing s
VMY Before
VMZ Flesh
VNF Protective
VNH Impossible
VOC Survey-lance
VOO Emplace ment
VOT During
VPE Bad
VPU Concentrate d ing ion s
VPY Spare 79
VQZ There
VRY Assault
VRZ Hyphen ( )
VSD Radiation
VSL Head-ed-ing
VTJ W
VTM Age
VTS Pris s of war
VTW Little John(LJ)
VTY Infiltrate g on
VUE Until (further notice)
VUM Tactic s al
VVN Indirect
VVP Offense ive
VVS Communicate d-ion s
VWL Attack-ed ng s
VXV Flexible-ility
VYC Cease s-d ing

W

WAB Wagon
WAD D
WAJ Azimuth (of)
WAY Paddy
WAZ Assist ance
WBA Outpost/post
WBH No/non/neg
WBL Ambush ed-ng
WBQ Spare 3
WBZ Spare 60
WCR M
WDC Going (to)
WDD Arm s ed
WDH Ot A(Bird Dog)
WDP Period ( )
WDV Perimeter
WEE Envelop-ed ing
WEM Telephone s
WEP Odor
WGD North-ern (of)
WGS Issue d ing s
WHP Agent s
WIA Ridge d-s
WIB Nothing
WIE R
WIP Brigade
WIS K
WIU To (be)
WJC Come ing
WJI Execute-ions s
WJY Unidentified
WKH Exhaust-ed ing
WKW Road s
WMQ Post s
WMT Guard-ed ing s
WNA Railroad s
WNU Swallow
WOC Troop s (lift)
WOP Market
WOX Spare 14
WPC UH 1D
WPJ Occupy ations
WPK 8MNT
WQE Miss ed ing

FOR OFFICIAL USE ONLY DECODE 7 KTC 600 A ISET 3

FOR OFFICIAL USE ONLY

WQL Over run
WQS Bypass d s ing
WRH Truck ed s ing
WRT Leaflet s
WSE Operate ion s
WSQ Separate d ion
WSW Spare 36
WTB Q
WUD Spare 54
WUF Spare 71
WUK Airhead
WVF Occupy ed ing
WVX Corps
WWA Commence d ment
WWG Internal
WWZ Restore s d ing
WXE Cut-off
WXO O
WXR Limit ed ing s
WYP Low er-est
WYQ Progress ed ng
WZA Concertina
WZC Up

X

XCB Aircraft
XCU Coord s d-ing
XCV M 16
XDC Intend-ed tion
XDH Spare 11
XDP Officer s
XDU Inform-d ation
XEF Hospital s
XFI It
XFW Target s
XFX Route s d ing
XHT Minimum
XIQ Breast
XJC Crane
XJF Blow ing (up)
XJQ Map ped png s
XJT Rendezvous
XKU Listen-ed ing
XLC Request-d g s
XLO Spare 98
XLS Spare 117
XMK 000
XML Spare 9
XNC Pick up
XNT Start ed ing
XPO Infantry
XPI Anti-
XPL Grid (coord)
XPM Headquarters
XPR Clear ed ance
XQG Total
XQH Bomb d r ng s
XRF N
XRG Stay ed ing
XRQ Contact-ing
XSI Terrorists
XTY 1
XUU Burst-ing s
XVA Result s ed ng
XVJ Spare 83
XVW Reorganize d ation s
XWD Spare 25
XWQ Attach ment
XXC Ty
XXO Spare 88
XXZ Element s
XYB Enemy
XZE ETA your loc
XZG Attack ed ng s
XZP Harass ed ing
XZS Spare 116

Y

YAC P
YAG Spare 84
YAH Incendiary-ies
YAK Echelon
YAS Psywar
YBT H
YCA Spare 109
YCJ Replace ment
YCU Depot (supply)
YCX Shell s ing ed
YDZ 000
YES Spare 115
YFF Defend ed g s
YFL Town/vil lage s
YFW Bomb-d r ng s
YGU Deputy ies
YGX Fight-er ing
YHK Resist-ed ance
YHL Penetrate ion
YHP Howitzer s
YHQ 1
YIH Amph-bious
YIK Hawk
YIP Extend d g ive
YIS Our
YJM G
YJO V (Fifth)
YJP 30 cal
YJQ Naval gunfire
YJV K
YKA Short ed
YKW Command post
YLR Of
YNL Conversation
YNO Down ed
YHQ Arrange d-ing
YOE Amputate
YOI No fire line
YQU Deadline d ng
YRJ My location is
YRZ Slow ed ing
YSH Remain ing
YSJ Exploit ed ing
YTB Superior ity
YTS Water
YUP Litter evac need at(coord)
YUQ Maintain ing s
YVI Approximate ly
YXD Add ing s
YXO Spare 98
YXP Emplace d ing
YYR Soldier
YZH Act as relay
YZN Spare 59
YZP Hand
YZQ Spare 6
YZW Z
YZZ Pipe line

FOR OFFICIAL USE ONLY DECODE 8 KTC 600 A ISET 3

TAC-OPS code is an extremely efficient method of written or voice communications. Developed for radio operations on the tactical (squad, platoon, company, and battalion) level, this code condenses the bulk of the message since every word is only three letters in length. Of course, if your operation employs words other than those listed, you must use the spare slots for more commonly used words and spell out any others.

For speed and security, a variation of this code can be developed by the operative to provide COMSEC for each cell. TAC-OPS code can be formatted into a one-time pad layout or grid code configuration quite easily. The one-time pad computer program can be utilized to assign a sequential group of five characters to a pre-established dictionary of standard words for message exchanges.

TAC-OPS codes are definitely amenable to certain cells more than others. An ADMIN/LOG cell has to handle a great deal of standardized equipment, materials, and so forth as part of its mission. Assigning certain items a standard brevity code is simple and straightforward. TAC-OPS code is not as useful for an INTEL/OPS cell due to the detailed nature of that cell's communications. Of course, targets, safehouses, locations, and operations can and should have their own brevity code words for basic security. All participants in the enterprise should likewise have their own brevity code identifiers.

After reviewing the TAC-OPS code on pages 89-92, the operative may wish to compose a message using the code and learn how versatile it can be. Further in this book is a section on monitoring military communications, and the operative will hear this type of code employed extensively in training operations as well as during actual missions. It is extremely useful to monitor this traffic and record it for training operatives in your organization.

Integrating TAC-OPS code into the COMMO plan has a number of advantages. Like all brevity codes and acronyms that are specific to an operation, they signifi-

cantly complicate matters for codebreakers. These codes can be employed wisely to create an expert code system that any cell could use with minimal risk.

MESSAGE PLANNING AND THE LIMITATIONS OF THE LANGUAGE

Regardless of the method selected for transferring a message and/or for creating a one-time cryptosystem, the operative must consider the text of the message carefully. He must take into account the nature of the language being used, as well as the ABCs of text traffic: ACCESS security, BREVITY of message, and CLARITY of message. Combining these simple concepts into a code system will provide an operation with a high degree of COMSEC.

It is important to understand the nature of the written language you are attempting to disguise as a code. In normal usage, the characters of the English language have a highly predictable sequence. Creative efforts focused on the elimination of predictable patterns are suggested.

There are a number of extremely common words in written English. According to the *American Heritage Word Frequency Book*, the twelve most commonly used words in written English are:

1. The
2. Of
3. And
4. A
5. To
6. In
7. Is
8. You
9. That
10. It
11. He
12. For

Although it would be impossible to attempt to communicate effectively without these twelve words, the operator should make note of them. If he can reduce the usage of these words by only 25 percent through the use of abbreviated text messages, the ability of the opposition to attack the code by computer will be degraded substantially. Habitual elimination of these common words, except when clarity is essential, will also greatly reduce the bulk text required for encryption. The same holds true for the eight most common letters in the English language: E, T, A, O, N, I, R, and S.

In an average message, over half of the words will begin with T, A, O, S, or W, and at least one quarter generally end with the letter E. Certain letters occur in sequence more frequently than others do. For instance, TH, AN, and HE appear most often together in English. ER, ES, and ED also occur together quite predictably. *Doubles* are another concern; the letters L, E, and S are often found together (as in the S in UNLESS). There are also common three-letter word groupings (called *trigrams* in the trade) that are found in most sentences. The four most common are THE, ING, CON, and ENT. If the substitution for any of these letters is learned by recognition of the commonality of their sequence, the code is that much closer to being broken.

Thus, it is important to recognize the limits of the language and incorporate a few "corrections" in your message before you actually encrypt the text with the one-time pad. Plan your plain-text message using the above guidelines and a few careful misspellings to create a more secure text message. Always start out with the complete message in longhand and then start trimming it down. For instance, consider the following message to be sent to an action cell commander:

BADGER. SAFE HOUSE FALCON IS OPERATIONAL. MAP AND DETAILS FOR THIS NEW LOCATION WILL BE FOUND AT DROP REDSTONE ON THURSDAY. CONFIRM THE RECEIPT OF THIS PACKAGE WITH A FALSE COL-

LECT CALL TO MESSAGE CENTER FOX IN THE NAME OF MARK GUNTHER THURSDAY NIGHT, BETWEEN 2115 AND 2215 ROMEO. DROP REDSTONE WILL BE SANITIZED FRIDAY AM. IF YOU HAVE TRAFFIC FOR ME, LEAVE DROP CODE DESIGNATOR AND TIME ON INSIDE OF AN EMPTY PACK OF MATCHES WITHIN TEN FEET OF DROP REDSTONE PRIOR TO FRIDAY AM.

First, the bulk of the text can be greatly reduced by eliminating almost half of the message without sacrificing clarity. Most obvious should be the use of the code name. If BADGER is to be the receiver of this message, it will be sent only to him for decoding; thus his name does not need to be on the document at all. In the second sentence, the nature of the contents of the drop known as REDSTONE is disclosed, and this is not only unnecessary but a breach of basic security as well.

For clarity, brevity, and security, the message should read more like this:

REDSTONE THURSDAY. CONFIRM THROUGH FOX COLLECT FROM MARK GUNTHER SAME DAY 2115-2215R. IF YOU HAVE TRAFFIC, ID DROP AND TIME AT REDSTONE ON INSIDE EMPTY MATCHBOOK WITHIN TEN FEET WHEN SERVICING.

Note that the sender now avoids telling BADGER when or even if the drop will be sanitized. Although he may intend on servicing this drop location and then making it inoperative somehow, BADGER does not need to know this, nor should he ever need to know when any drop is to be serviced. Remember the ABCs of sending covert text. Is ACCESS to this information critical? If not, delete from the message. Is the message written with BREVITY? Keep it short. Finally, is the message CLEAR? Remember: ACCESS, BREVITY, and CLARITY. ABC. In the above example, the message is kept the same, unnecessary access is eliminated, and the volume of the text is cut well over half.

Finally, the limitations of the language can be

addressed. Understanding what words and character sequences to avoid, the message would then progress to something like this:

REDSTON TH. CONFRM 2 FOX COLEKT MARK GUNTHER TH 2115-2215R. IF U HV TRAFIK ID DRP ON MT MATCHBUK WITHIN 10 FT REDSTON TH.

The key factor here is uniformity of format. The reader of this message should be familiar with the use of certain brevity codes just as intimately as he should know where the drop known as REDSTONE is. Brevity codes make the encryption of text faster since the message bulk is reduced, and a high level of security is placed on the inherently risky use of the written word.

Brevity codes are useful in the initial stage of plaintext conversion because the opposition will attempt to attack the code without specific knowledge of the use of these simple additives. In the above example, the word EMPTY has been replaced with MT. There are a number of other options available:

ARE	R
TO, TOO	2
YOU	U
SEE, SEA	C
FOR	4
BUSY	BZ
BEFORE	B4
FORM	4M
EASY	EZ
TO BE	2B
SEE YOU	CU

These codes are fairly straightforward. There are dozens of others in one-, two-, and three-letter combinations, all of which will quickly degrade an opponent's ability to attack the code. They will be looking for doubles and trigrams in the text, and if they are avoided, the

computer system has to employ other strategies. Be imaginative and the entire code will be very hard to break.

• • • • •

Guerrilla cryptography in a small cellular unit is seldom very sophisticated. Unlike "days of old" when large nations sponsored dozens of guerrilla operations around the globe—providing some advanced communications systems to many of them—the modern scenario is frequently much more fluid, requiring the guerrillas to devise and develop an internal COMSEC plan using indigenous materials. Available off-the-shelf technology and field-expedient techniques can provide excellent security.

As has been stressed in this chapter, the fact that a written or transmitted message is in code is highly incriminating in itself. Even if the opposition is temporarily unable to break the confiscated message, this is seldom any consolation to the individual caught with a coded message in his or her possession. Keep this in mind as you consider various codes and the attendant paraphernalia involved with making and sending them.

7 ● VOICE COMMUNICATIONS

Underground operations require constant and instantaneous access between command, operational, and support elements. The primary means by which this is accomplished is through voice communications media. *RATELO* (radio and telephone) systems are exploited to provide command with the ability to interact with various elements on a real-time basis. The main features of voice communications are:

1. SPEED. No other communications means is faster or allows more instant access to all team elements in a manner that permits the commander to quickly make and implement decisions as a situation develops. Voice also allows instant confirmation of reception and comprehension of instructions.

2. FLEXIBILITY. Radio and telephone systems can be integrated as the main part of a COMMO plan as well as serve as backup for one another. For the most part, these systems are already in place in the target area and the exploitation of commercial circuits is quite simple.

3. SIMPLICITY. RATELO communications require minimal training, manpower, or financial resources, and can be quickly set up and operational in the target area as needed.

There are operational considerations for utilization of

either radio or telephone communications systems. Each approach has limitations.

TELEPHONE COMMUNICATIONS

Telephone systems are in place and operational worldwide. If the operative has a small, portable uplink system, the international communications satellite system (COMSAT) allows access to commercial telephone circuits from anywhere on the planet. Long-range high-frequency (HF) radio telephone units allow ships and aircraft to make use of these telephone circuits as well.

For the typical underground operation, access to a telephone does not require such sophisticated hardware—a reliable voice communications system with worldwide access is as close as the nearest pay telephone. Because of the simplicity of operation, universal reliability, and general ease of long-range operation, the telephone is used by many underground groups as the primary means of communications.

This chapter will focus on expedient methods to gain access to the commercial telephone system anonymously. There are a number of reasons why simple installation of service is not practical for many operatives. The need for mobility, quick access, and a degree of security is a consideration when deciding to employ the capabilities of telephone communications as an integral part of the communications plan.

The significant advantages of telephone communications are that telephones generally are more secure than radio and are extremely reliable, and exploitation of commercial circuitry already on-line requires minimal equipment or time. The telephone system in your target area can be exploited and continuously used to maintain contacts worldwide. It can also be employed to send data, image, and bulk text quite easily. In fact, even funds can be sent using the telephone system. The

only problem with using telephone communications as a covert tool is security.

Telephone Communications Security

Before discussing specific methods and techniques of exchanging information via the telephone, it is important for the operative to have something completely clarified. Telephone conversations are *not* secure. This should seem obvious to any experienced operative; however, the commercial security market has become deluged with technologies, devices, and contraptions that purport to provide a secure means of using the telephone to communicate sensitive information.

Most nations and many individual jurisdictions employ a variety of methods to intercept, record, and analyze telephone traffic. The U.S. National Security Agency (NSA), for example, is tasked by congressional order to intercept, monitor, record, analyze, and file *all* overseas telephone conversations that originate or terminate within the United States. Telephone conversations are intercepted and computer analyzed for voice characteristics, previously filed or flagged voiceprints, and so forth.

The NSA's modern supercomputers can handle thousands of conversations simultaneously around the clock. The monitoring system can electronically identify the voice characteristics and even the identities of both parties and log both the number called and, if originating in the United States, the number used to initiate the call. To a certain degree, it can electronically analyze the content of the conversation without any human involvement whatsoever, which permits the agency to literally sweep through any phone system and gather all critical information cheaply and efficiently. The computer will notify the NSA operators if the voiceprint, the particular numbers called or used to originate the call, or the content of the conversation may be of some use to the intelligence requirements of various agencies in the U.S. government.

Incidentally, the transmission of data, fax, or scrambled voice communications automatically receives priority. The computer analyzes it immediately, notifies the operator, and even descrambles any type of encrypted traffic.

Many intelligence and law enforcement agencies intercept domestic telephone conversations on a large scale using microwave intercept equipment. Every major city and town uses either microwave or fiber optic equipment to route telephone traffic. To intercept these conversations is somewhat sophisticated, but it is not beyond the scope of any operative to conduct such an operation.

The point of this brief section is to emphasize that *no telephone line is secure.* If someone tells you they are on a "clean" or "secure" line, they are either lying or they are extremely naive. No electronic gadget or device made, no "sweep" conducted, regardless of how professionally done, can provide a 100-percent guarantee of telephone security. Consequently, rule number one of telephone COMSEC is that all operatives must *assume* the conversation is being recorded by the opposition and adjust the conversation's content in a manner that eliminates the possibility of the operation being compromised.

Sophisticated and expensive gadgetry for telephone security such as scramblers, voice alteration devices, pocket-size "tap detectors," and tone-burst data communications systems are not only simple to defeat and somewhat amateurish to employ, but they actually call attention to your conversation instead of providing even a small degree of security. Many books and publications exhort the technical and security capabilities of these devices, but the technology is now extremely dated and in fact counterproductive to efficient COMSEC. This book advises against the use of these devices for a couple of simple technical reasons.

Any electronic device that is intended to encrypt, encode, or electronically alter telephone communications must do so within the electronic frequency-response

parameters that are available through the normal telephone system circuit. Basically, this means that the alteration or encryption must use a very narrow section of the audio spectrum in order to function. What this means to your opposition is that any such traffic can be intercepted and recorded anywhere along the path that the signal travels and then computer analyzed. So the very existence of this type of electronic alteration is not only instantly detectable, but also capable of being decoded.

There is no commercially available technology that is beyond the decoding capability of the government agencies tasked in the interception and analysis of such traffic. Since the inception of computer-assisted microwave and satellite uplink intercept technology, all telephone traffic that contains scrambled, encrypted, or altered content is immediately "flagged" and usually decoded on site. It is *always* recorded. The point is that such conversations are now an excellent way for you to call a great deal of high-level attention to yourself.

Pay Phone to Pay Phone

If your target area is a major urban setting, there are literally thousands of pay telephones that can be used to communicate reliably. The most significant advantage of using a pay phone is that the volume of unrelated phone traffic makes a tap on one subject or group of subjects expensive and time intensive. The previous section should give the operative a basic understanding of the risks involved with using the pay phone or any telephone in exchanging compromising or incriminating information.

A series of pay telephones within convenient proximity to your residence or safehouse can be utilized to conduct communications with a degree of safety. This approach requires you and each operative in your net to create and maintain a personal pay phone directory with location, phone number, and call sign for each phone. If you explore your area, you will have no trouble finding at least a dozen

phone booths within close walking distance in any urban setting. The selection criteria for a phone booth should take into consideration such factors as proximity, twenty-four-hour access, shelter, lighting, and privacy.

The booth's phone number should be on the phone's dial pad. If it is not, try dialing #200 to learn the number. If the number is not available and #200 doesn't work, then the following measure must be taken.

Safehouse FALCON • 201 D Street • Anytown, USA • (501) 555-1212
Pay Phone Directory

Phone	Number	Call Sign	Location
A	555-4321	Amy Able	C & Wall
B	555-3214	Bob Bane	D & Wall
C	555-2143	Carl Cam	C & 2nd
D	555-1432	Don Deal	1st & D
E	555-4433	Ed Eagle	2nd & E
F	555-2211	Fran Finn	Wall & C
G	555-1234	Gwen Gold	Wall & E
H	555-2341	Hal Henry	Wall & B
I	555-3412	Ida Ingle	E & Main
J	555-4123	John Jenks	B & 1st
K	555-3322	Ken Keest	Main & B
L	555-1133	Lily Lakes	Main & D

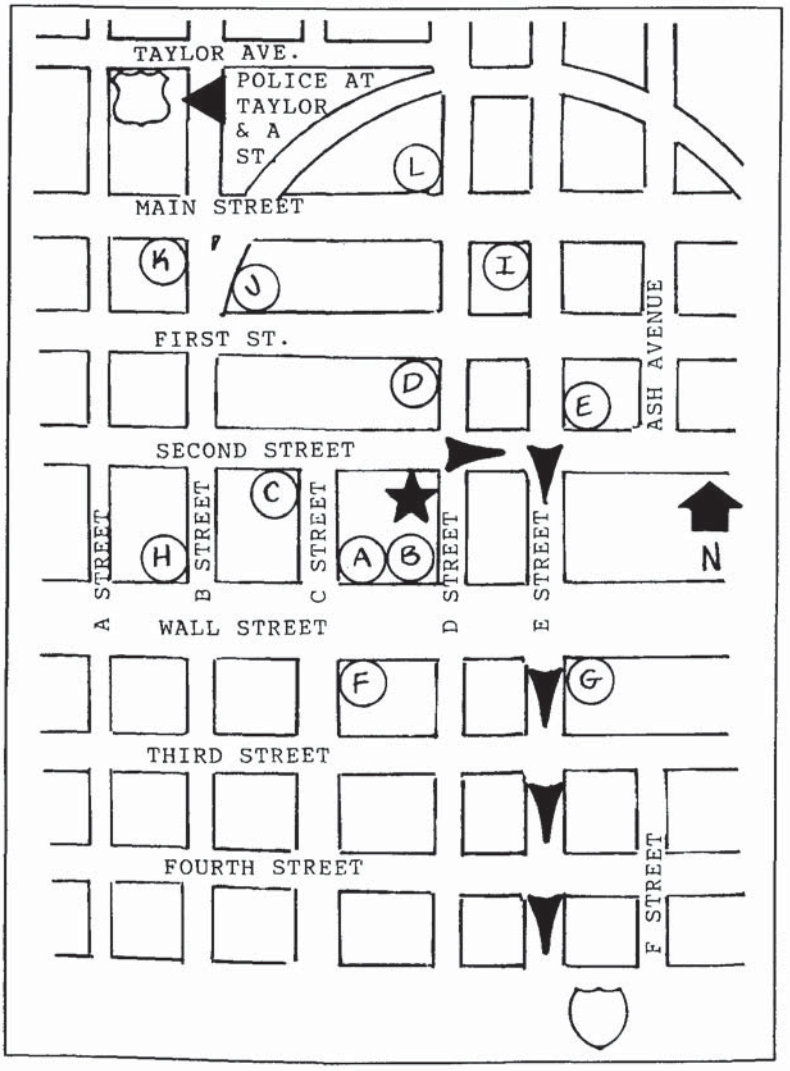
Signals	Call Sign
Urgent	Jerry Lent
Abort	Andy Burton
Compromised	Carl Mise
Shut Down	Bob Claus
Leave Now	Leo Howell

Operating Instructions

Answer on second ring only!
Authenticate.
Ask operator to repeat collect call names (To and from whom?).
Advise operator politely that it is a wrong number.
Log both names and time call came in.
Never accept any charges.
Never make calls on this phone.

Notes: Police Dept. at Taylor and A.
Interstate on-ramp 5 blocks south on E (primary escape).

Have a friend stand by at a residential phone and call him collect from the pay phone. When the operator makes contact, have your friend say that the person you are trying to call just stepped out, but if the operator can leave a number, he will call you right back. The operator will tell your friend the number of the phone booth.



Simply calling the operator and asking which number you are calling from sometimes works, too, although for internal security reasons many operators are not permitted to give this information out.

Let's examine how a pay phone directory could be used at a safehouse. In most underground operations there is a need for constant mobility for at least a portion of the operatives. This requires a covert network of supporters or sympathizers who will provide temporary residence for personnel active in an operation or who are in fact "wanted" by the authorities for one reason or another. The owners of the safehouse need to be protected from details of the operation, and no communications, activities such as meetings, or weapons or equipment storage can be conducted from the safehouse. The cell commander must have a means of contact with the occupants of the safehouse, but this can be accomplished by using the safehouse phone as a "message indicator" only and a number of pay phones close-by for actual message transfer.

When an operative arrives at the safehouse, he needs to be briefed on the area and the rules for living there. The operative is provided a detailed local map as well as a hand-drawn map of the immediate area, as in the illustration. All essential details are provided on the map, including the pay phone directory, a primary escape route, and the location of the nearest police station.

At safehouse FALCON, the directory, map, warnings, and communications signals and protocol are outlined on one sheet as part of the operative's initial briefing. This sheet could also be issued as part of his assignment to go to this city and set up at safehouse FALCON. Command should have a copy of this document as a means of establishing contact with the safehouse.

The pay phone directory includes the physical location of the pay phone, its phone number, and a call sign. The pay phone call sign should be a name that can be

clearly understood over the phone. In the illustration, pay phone A is designated "Amy Able" and is located at the corner of C and Wall streets. This phone is around the corner from the safehouse.

A collect call from "Jerry Lent" to "Amy Able" means that at a prearranged time the operative should be at pay phone A for an urgent message. If any call comes in collect from "Leo Howell," all personnel are advised to leave the safehouse, split up into small groups, and go to alternate locations or whatever has been prearranged. (This "leave now" signal can be sent from a pay phone in a jail cell or from anywhere in the world without the sender having to actually pay for the call.)

Safehouse FALCON uses the pay phone directory to maintain contact with other cells and individuals involved in the underground op. The telephone in the residence is used only to receive the message indicator—it is *never* used to originate or conduct message transfers. When it is necessary to contact an individual at safehouse FALCON, command knows the communications protocol to call the desired operative at a predesignated pay phone on the sheet.

The actual owners of the safehouse may or may not reside there. As long as the occupants understand the protocol, there is no need for nonessential personnel to be there. The safehouse phone must be manned twenty-four hours a day so command can access all personnel who are either there or close-by. Note also that the operating instructions state that the phone must be answered only on the second ring. This is a low-level authentication method that helps the caller verify that he has reached an occupied safehouse. If the phone is answered on one ring or three or more rings, it is a distress warning signal to alert the caller.

The pay phone directory concept can also be employed by a small operation of only a few individuals. All of the same rules apply. The safehouse may be the resi-

dence of one operative who acts as a *cut-out* between the operatives in that city and the rest of the cell. The safehouse is nothing more than a center to transfer and exchange communications on behalf of a group of individuals. The point is to have a phone accessible to initiate contact and to inform the caller of priority messages, emergency warnings, and the number of a "clean" pay phone to make the contact on. The approach can be conducted so that the initial collect call appears to be a "wrong number."

As with the safehouse, the phone at your residence should never be used to conduct message exchange. As you become more active in an underground operation, you will find yourself extremely mobile. You may have to reside in a series of temporary safehouses in order to avoid detection, enhance operational security, or avoid an active effort aimed at your capture.

Pay Phone Limitations

The long-distance network of AT&T has control over most of the pay phones in the United States. There typically is a flat rate to call any long-distance number in the country from a pay telephone. (In the spring of 1991, it was $2.05 for business or peak hours and $1.95 for off-peak hours for the first minute of calling.) This rate seems to apply if you are calling inside the state to another area code or clear across the country.

Certain underground groups train their operatives to carry a roll of quarters ($10.00) and to call only from pay phones to some prearranged message center to exchange information. But there is a problem with this strategy that seems to have been overlooked. Simply because a pay phone user deposits coins into the phone to place a long-distance telephone call does not mean that a toll billing record is not generated. In fact an internal billing record *is* generated. This is very important to consider.

For example, you are involved in an action in a spe-

cific city. You leave your hotel or safehouse, walk to a nearby pay phone, and call your base or main message center. You deposit the coins, make a forty-five-second contact, hang up the phone, and never use that pay phone again. Good COMSEC? Not really. If you or your group are suspected of being involved in some activity in a target city, and if the location where you stayed can be approximated, the authorities can quickly check the toll billing on *all* pay phones in the general vicinity of the area by computer and determine if calls were made to your message center during the times in question. Finally, after reading the section on telephone communications security (pages 101-103), it should be obvious that conversations using pay telephones are fairly simple to intercept.

Paying for the call by coin is only secure when you are calling another pay phone that no one in the cell will ever use again. On the other hand, if you use a telephone credit card to make the call and the long-distance carrier's 800 number to initiate access, no record is kept on the pay phone toll accounting system. In fact, all that can be determined is that the call originated in the specific city. As you will see in Part III of this book, the actual "account" used to make the call is in no way associated with you or your cell.

RADIO COMMUNICATIONS

Radio communications are the fastest way to get a message to a specific group or individual. Radio is useful when conducting any type of raid or ambush. A radio link with an early warning system is indispensable when conducting a covert penetration of an area or building. No operational cell should attempt to conduct a high-speed entry or urban raid without a radio link. Though there are a number of underground activities where radio is critical, there are also a number of threats in the use of radio as an integral part of the communications plan.

Radio is the least secure means of communications. Radio signals can be intercepted, jammed, and even deceptively altered by a technically proficient opposition. Do not overlook this threat. Underground operations or guerrilla warfare will almost always be conducted against a physically and technically superior force. Your radio traffic will not only be identified, but your physical location will be pinpointed in the process. Irresponsible use of radio communications can function as a literal homing beacon on your operation.

A fairly good rule of thumb in formulating a COMMO plan is that if there is any means of communications *other* than radio for a specific application, use it. With that said, there are a number of fairly safe applications for radio communications, and these will be discussed in detail.

One-Way Radio Link

Underground ops frequently require clandestine access to an individual or group that is not at a specific geographic location. The cell is tasked with maintaining itself undercover in a given area, training and practicing its specialized skills in a manner that draws no attention to itself. To covertly control this type of cell, the *one-way radio link* (OWRL) is an excellent option.

The agents of the cell are provided with radio receivers capable of picking up a specific frequency. At a preset time, the command net sends out an encrypted voice transmission over this predetermined frequency from an area outside the target region. The agents within range of the transmission can receive instructions and messages from command fairly anonymously this way.

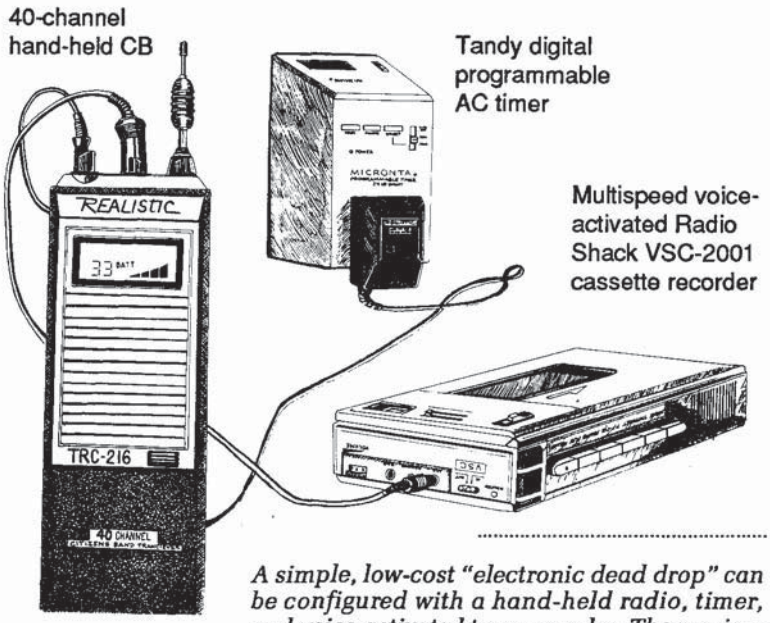
For example, an age-old technique (employed by both sides during the Cold War and still used today) is clandestine *numbers station* broadcasting on the high-frequency shortwave band. These stations can be received anywhere in the world. The broadcasts are simply a series of number groups, generally five digits long, which

are broadcast at a specific time and directed toward an agent or cell in a target country. The nature of high-frequency propagation makes the origin and intended destination of these transmissions open to speculation.

The broadcasts can be heard on a number of shortwave radio frequencies throughout the day in North America and Europe. The numbers are read off by a male or female or by computer voice recordings in a number of different languages. Intelligence agencies and even hobbyists listen to these broadcasts and record them for reference and study. Some voices become familiar, as do certain frequencies and formats of numbers. Although volumes have been written regarding the origins and intentions of numbers stations, the fact is that unless the listener can understand the content and meaning of the code, the ability to intercept the transmissions does little good.

An underground organization can employ the numbers station technique and one-time pad encryption to communicate on an international level with a large or small cell. All that is required is a radio transmitter of the desired range and the capability for the cell to receive the transmitted frequency. A one-time pad or TAC-OPS code is an excellent means of using the one-way radio link as a fairly secure part of a COMMO plan.

Any device that can transmit radio signals can be utilized for this approach, including amateur radio equipment and low-cost FM radios. With a little preplanning, an ordinary citizens band radio can be employed. For example, command arranges to transfer encrypted number groups to all cell members late at night. Each agent connects a low-cost timer to a CB walkie-talkie with an AC adapter to turn on both the receiver and a tape recorder at the designated time on the designated CB channel. In this configuration, the agent does not have to wake up to receive the message or even be at the location where the radio and timer are set up when the message comes in.



A simple, low-cost "electronic dead drop" can be configured with a hand-held radio, timer, and voice-activated tape recorder. The receiver of the message simply programs the timer to turn on the CB radio and recorder at a specific time. Using a variable-speed recorder such as the one illustrated allows the sender to transmit messages at two to three times the "normal" speed of a voice message. (Illustration courtesy of Mark Camden)

This approach allows command to contact a number of cell members in a given area and distribute messages and instructions fairly quickly and securely. Using a grid code for text message transfer allows a number of cell members to receive the message, but only those individuals specific to the message will be able to decode the text. Additionally, the cell commander can send the coded transmission from a mobile unit or set up the transmission to occur with a timer, similar to the receiver arrangement.

The advantage of using a OWRL is that the transmissions can be sent quickly; the target simply receives the transmission and is not at risk of being compromised by transmitting himself. Another advantage is that the opposition can have a great deal of difficulty locating the

source, content, and target of such communications. The imagination of the communications officer and the available hardware are all that's required for a successful link.

The risks of employing this approach are also numerous. Possession of the transmitting equipment in a denied area may be illegal. Furthermore, the agents or cells must be versed in decoding the traffic, oftentimes needing certain hardware and one-time pads to receive and decode transmissions.

The most significant applications of the OWRL are in the use of powerful transmitters outside of the enemy's region and reach that broadcast encoded messages to small receivers inside the target area. There are a few options for the underground group to employ, and though they are illegal and certainly unethical, they can help reduce the risk and peripheral costs involved with employment of the OWRL.

Bootleg Voice Paging System

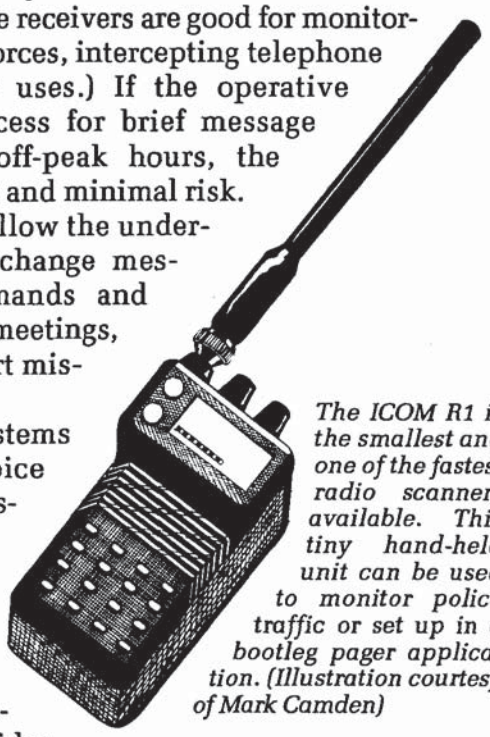
The transmitter is the most expensive part of a COMMO plan that utilizes a one-way radio link. Guerrillas often steal the necessary hardware for this application, but modern technology offers a fairly clever alternative. You can simply "borrow" a transmitter in the target city and access it from anywhere in the world.

You do not want to get caught performing the following technique. It involves a serious though seemingly harmless theft of a commercial radio paging service. The concept is fairly simple and the results are quick, but the owners of the paging system certainly will frown on this approach. Read this section completely to understand the risks involved.

There are millions of radio pagers in use throughout the world, and every city in the United States has pager transmission systems in place. Radio pagers are used by doctors, police officers, attorneys, technicians, and other professionals. Drug dealers and other criminals also have

found these small radio receivers useful in the conduct of their business.

By programming a radio scanner with the common radio pager frequencies (pages 118-120), the operative can intercept these transmissions and gain enough information to use the pager and a scanner together as a communications tool. (Every cell should have at least one radio scanner. These receivers are good for monitoring local security forces, intercepting telephone traffic, and other uses.) If the operative bootlegs pager access for brief message transfers during off-peak hours, the approach has merit and minimal risk. This strategy can allow the underground cell to exchange messages, send commands and warnings, arrange meetings, and initiate or abort missions in seconds.



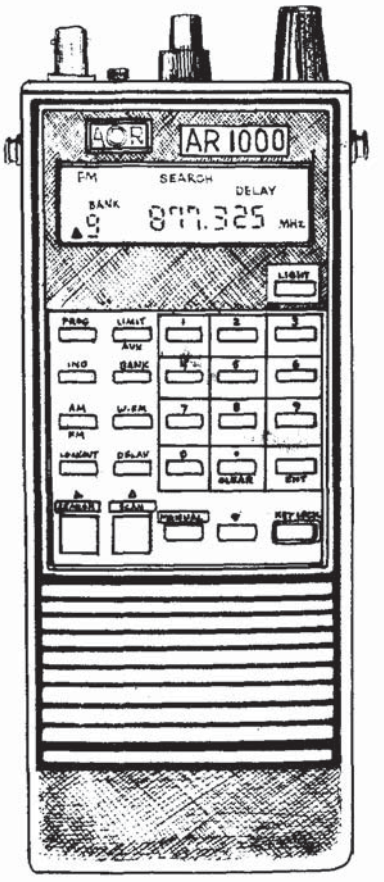
The ICOM R1 is the smallest and one of the fastest radio scanners available. This tiny hand-held unit can be used to monitor police traffic or set up in a bootleg pager application. (Illustration courtesy of Mark Camden)

Radio pager systems can send both voice and data transmissions. Data transmissions generally are a series of tones that send a digital message to the specific pager. The pager provides the subscriber with a digital readout of the number he is supposed to call.

The other less common type of pager is the voice pager, and this is the one of interest. When the voice pager number is called, the caller can leave a verbal message for the subscriber. This voice message, typically from twenty to sixty seconds in duration, is then transmitted over the airwaves along with the access number to actuate the spe-

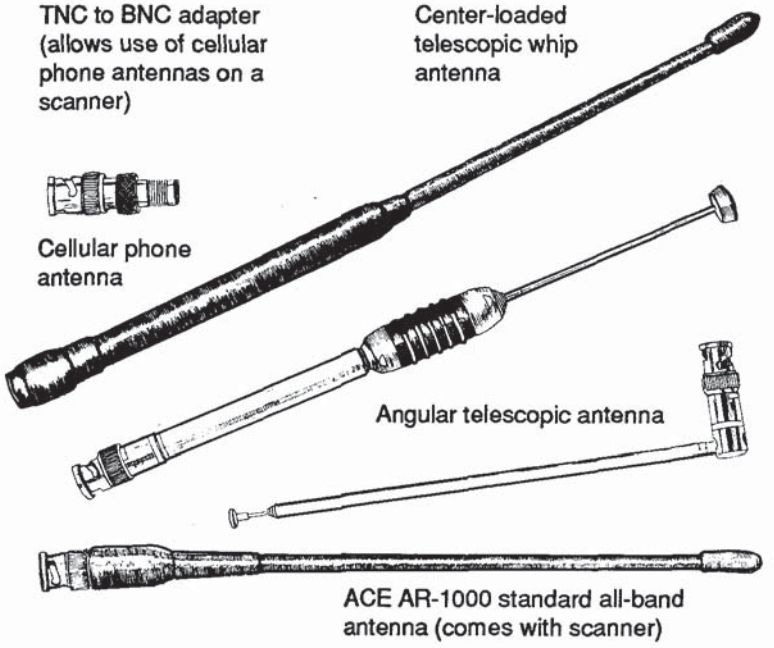
cific pager intended to receive the message. Using a scanner programmed with the pager frequencies, the operative can intercept and make note of these voice messages to gain access to the pager transmitter.

Monitoring the radio scanner for less than an hour generally will result in the interception of a number of voice messages, such as "Tom call Jerry at 555-1234." As soon as you intercept this message, make note of what pager frequency you heard the transmission on and immediately call the number on the message. When the person answers, tell them that you work for some well-known local company and your pager has been going off all day with their messages. Politely ask the person what number they are dialing to page the person they are calling so that you can report this to



The ACE Communications AR-1000 scanner is the ideal underground communications intercept unit. With a 1,000-channel memory and 10 search banks with interchannel lockout, it has the highest channel memory capacity of any hand-held scanner sold in the United States. The frequency coverage of 8-1,300 Mhz allows the unit to receive standard shortwave broadcasts all the way up to microwave pages, airphone traffic, and virtually all voice radio communications in the spectrum. (Illustration courtesy of Mark Camden)

the pager company. The person who initiated the page will almost always give you the pager phone number, at which time you have gained access to the specific radio transmitter frequency keyed into your scanner. By calling the pager number, you can transmit your voice message all over town to anyone who has a scanner tuned to this frequency. By monitoring a while longer, you can use the same approach to collect a number of telephone pager


TNC to BNC adapter (allows use of cellular phone antennas on a scanner)
Center-loaded telescopic whip antenna
Cellular phone antenna
Angular telescopic antenna
ACE AR-1000 standard all-band antenna (comes with scanner)

A variety of antennas available for the AR-1000 scanner for use in intercepting telephone traffic. (Illustration courtesy of Mark Camden)

access numbers, giving you a choice of reliable, fairly long-range one-way radio links.

In many cases, pager transmitters on the VHF frequencies can send page signals for more than 100 miles. The communications officer can call the pager number from a distant city and relay a brief voice signal to all cell

members in the target city by having a prearranged time to have the scanner tuned to the pager frequency. The voice message must be brief and sent late at night to prevent the legitimate subscriber from discovering the illegal use of his pager number, as well as for the cell members with scanners to avoid having to listen to the "clutter" of other messages heard during the day.

There are many situations in underground operations where the bootleg pager can be a major benefit. If a new operative is to link up with a certain cell or agent in a target city, he can be instructed to arrive there by a certain time and go to a specific pay telephone. After being observed at this phone, he can call the pager number and give a password over the pager. This can establish the legitimacy of the operative prior to any members actually meeting him.

Pager access can be used as an early warning system for active cells. Many radio scanners have a *priority* function that programs it to sample a specific radio frequency every two seconds for any traffic. A cell can use this function late at night when monitoring security or police forces—if the message frequency is programmed in the priority channel, the scanner will immediately go to that channel to receive the traffic when the pager is activated.

Pager bootlegging can transfer long-distance credit card numbers (more on this later) to a specific cell in a target city or exchange other encrypted number transmissions, as long as they are brief. Credit card numbers should be sent in some sort of encrypted manner, since radio voice page transmissions are recorded by the pager company, at least temporarily. They are also subject to intercept by other scanner owners, although this is actually quite rare.

Using this technology and a small amount of practice, the communications officer can travel with his team to a strange city anywhere in the world and instantly have access to a OWRL for citywide communications. Pager

bootlegging has all the benefits of a covert OWRL without possession of the transmitter. This technique can be an excellent communications strategy for an action cell, and if recording equipment and a timer are connected to a scanner, the pager bootleg strategy can function as an electronic dead drop for exchanging signals or brief messages very securely.

The operative should *always* avoid bootlegging on medical page frequencies or those likely to be used by anyone late at night, such as for undercover police work. Medical pagers typically operate on their own allocated frequencies or are obvious since the voice page message generally instructs "Doctor ___" to call extension "___," or something to that effect. Do not disrupt medical page traffic; lives may be at stake. Simply monitoring pager frequencies on a scanner will reveal certain pagers employed by maintenance people or technicians that are unlikely to be used late at night. These pagers are ideal for a COMMO plan.

The following are the frequencies for radio pager (sources: *Tune in on Telephone Calls*, 1988 by Tom Kneitel K2AES; *Police Call Radio Guide*, 1991 by Tandy Corp.):

Medical and Emergency
(Do not use these frequencies for bootlegging!)
35.640 Mhz
35.680 Mhz
43.680 Mhz
152.075 Mhz
157.450 Mhz
163.250 Mhz

Business and Professional
152.480 Mhz
154.625 Mhz
157.740 Mhz
158.460 Mhz

72.020 Mhz-72.980 Mhz
75.420 Mhz-75.980 Mhz
152.000 Mhz-152.840 Mhz
158.100 Mhz-158.900 Mhz
929.000 Mhz-932.000 Mhz

Two-meter ham radio transceivers, marine band VHF radios, and a number of business-type walkie-talkies can also be employed with a scanner to function as OWRLs. If the agent keeps the messages brief, transmits from a secure location, sterilizes the area after transmitting, and never transmits from the same location twice, the OWRL provides a degree of security that many types of radio are unable to give.

Overall, the use of radio is very risky in covert ops. It is simple to intercept radio traffic, and even scrambled or "secure" transmissions do nothing to prevent the operative from being located with *radio direction finding* (RDF) techniques, which, with the help of computer technology, are fast and accurate. Being captured with possession of the hardware described in this section would be very unpleasant if it could be linked to illegal activities.

Radio monitoring with scanners and receivers should be encouraged for all members of a cell. Studying and understanding the opposition's radio traffic can be a great help in avoiding confrontations. My book, *Improvised Radio Jamming Techniques: Electronic Guerrilla Warfare* (available from Paladin Press), provides detailed insight into this very interesting strategy.

8 ● DISSEMINATING INFORMATION

Oftentimes a communications plan can benefit by having the capacity to not only collect and exchange information but also circulate a specific message to the masses. A target audience must be studied carefully and understood before attempting to "reach" it covertly. It is useful to have access to the masses for recruitment and to influence opinions. It is also quite dangerous to do so.

Obviously, your audience should have access to the medium you select to convey the message. Again, exploitation of available media can have the desired effect. In fact, the most useful means of communicating an unpopular or controversial message to a mass audience is to make the delivery itself equally controversial. When properly employed, bootlegging or pirate activities become news stories themselves. With a little imagination, you can exploit the existing communications media to assist you in reaching a mass audience.

For example, your group may wish to direct attention to a specific incident or atrocity committed by the opposition that has not been adequately covered in the press. One group in California did just that when it decided that the media coverage of the war in El Salvador was slanted and unfair. The group felt that the media was as much to blame for the problem as the actual policymakers in

Washington. Their solution: they printed a bogus copy of the front page of a large local newspaper, even using the paper's masthead, covering a number of military atrocities alleged by the group to have been committed by the El Salvadorean military. These bogus front pages were secretly placed on the Sunday edition of the paper inside hundreds of vending machines.

Many readers thought that the newspaper actually printed this "insert," and in fact, the paper had to print a disclaimer. Furthermore, this inexpensive, clever approach gained the attention of the national media.

This is an excellent example of making the act of communicating the opinions of an underground operation as newsworthy as the opinions themselves. By using creative and perhaps unconventional approaches, the content of your message becomes almost secondary to the medium you employ to disseminate the message.

The following are some examples of how an individual or small organization can disseminate information in a manner that covertly gains access to the masses while calling a bit of attention to its cause from the media.

CREATIVE INSERTION

The example of the newspaper insert is useful, and you may want to consider it. Another approach that might generate a bit of attention would be to rent a large number of videocassette recordings of popular movies and momentarily override the record protect tabs to record your message somewhere in the movie. This can be devastating if you employ the right images at the right time in the right movie. In a popular action adventure movie, the climax of the film can be interrupted with your home-produced images. An animal rights group, for instance, can show the methodical slaughter of some breed of fur animal at this point for excellent effect.

The advantage of this approach is that the attention of

the audience is guaranteed. They are shocked by the interruption, which of course makes them very irritated and upset. They will not forget this incident. The viewer will likely contact the video rental store and demand a refund, and the business will likely demand an investigation, which may get the attention of the local TV and print media, particularly if the message is put on a number of videotapes and the content and quality of the message is such that a number of people call attention to this rude interruption of their entertainment. You can get the ball rolling by calling the city desk of the target papers and TV stations with a "tip" about the story.

Another even more illegal approach would be to "borrow" the bulk mail permit of your opposition to do a creative mailing of your own. Printing duplicates of the OPFOR's stationary and envelopes and sending out a large number of inflammatory messages will certainly get a lot of attention from the target group and the media. Sending illegally produced mailings with an unauthorized bulk mail permit would cause quite a stir, and the reader should be advised that the investigation that would follow would be very aggressive indeed.

Again, the key element in creative insertion is understanding that the conduct of the communication can be as newsworthy as the actual message. The environmental group Earth First!, for instance, plasters messages on billboards, covers up the advertisement, or simply drops the billboard to the ground with chain saws. This is in protest of the "land rape" caused by the billboard company. This approach is clever, innovative, and certainly easy to do.

The more effective "communiqués" all seem to employ media that are somewhat unconventional in nature and generally are conducted in the form of a prank or a ruse. It used to require a barbaric form of violence or terrorism in order to gain national media attention. Many groups now employ a much different approach—they seize the medium only for a brief moment to get the message out.

Remember, your opinions and objectives may seem to you to be realistic and for the betterment of society, but this has no bearing on whether anyone will chose to listen. Therefore, you want to accomplish the following:

1. Identify the situation in a manner that gets a lot of attention. Turn apathy into emotion.
2. State the facts in a manner that will influence opinions.
3. Access the masses in a manner that cannot be ignored by the media.

You can certainly operate just outside the law to communicate your message effectively; just be cautious and clever. The more you seem to defy the system, the better your chances that people will observe or listen to your message. Don't hesitate to generate negative emotions from your target audience. When you interrupt the apathetic, they tend to get a little annoyed. That is fine. In some cases it can be beneficial.

PIRATE OPERATIONS

Creating a media center with pirate radio or television stations offers great opportunities. The fact is that for a couple hundred dollars, a video transmitter can be had that can transmit for miles on one of the normal TV channels. A video transmitter in kit form can be purchased from North Country Radio, P.O. Box 53, WYKAGYL Station, New Rochelle, NY 10804.

Pirate TV and radio broadcasts are, of course, very illegal and require a covert approach to get away with. Pirate broadcasting in the United States is becoming a serious activity, and the Federal Communications Commission (FCC) is becoming very aggressive in attempting to halt it. Still, the creative and imaginative application of technology in a manner that seems to attack or subvert the mainstream media tends to gain a lot of attention.

Should your group wish to look into pirate activity, there is one source for all the facts and hardware needed to conduct this risky enterprise safely: PANAXIS, P.O. Box 130, Paradise, CA 95697.

A pirate station should be controversial and entertaining. It should be an alternative to the general media. This often can be accomplished by jamming the broadcasts of popular stations, and the equipment needed to do this is the same equipment required to broadcast your own message. Imagine two or three TV stations getting jammed at the 6:00 P.M. news broadcast and, one station over, your little pirate video station giving the viewer a whole new perspective of the "news on the hour." This would require careful and elaborate planning, but the results would likely gain national attention to your cause.

Even Third World nations have a large number of television sets and radios per capita. If the language and the audience are understood, a covert operation can access the masses with a pirate broadcasting station more easily than with underground newspapers or leaflets.

In general, the media in most countries are either a propaganda tool for the government or a means of generating revenues for a company. Accept this reality and exploit it. Force the medium that is ignoring your cause to disclaim the insertion of your message or the interruption of its programming. Be clever. Cheat, steal, interrupt, and insert your message among the media already accessible to the target audience. Make your message and your method newsworthy by breaking the "rules" of the game.

PART III

TECHNICAL ASPECTS OF UNDERGROUND COMMUNICATIONS

9 ● TELEPHONE SERVICE THEFT AND FRAUD: A HISTORICAL PERSPECTIVE

The telephone is one of the most basic essential tools in an underground communications plan. Using the complex international telephone system covertly often involves the theft of telephone service.

It has been reported that the theft of phone service is done for economic reasons by the international "underground community"—criminals, mercenaries, terrorists, political outcasts, fugitives, informants, and intelligence operatives. That is only half the story.

This final section of the book will explore dozens of methods to make a "free" telephone call. The concept is neither new nor innovative in underground operations. Yet the reason this approach is so effective and popular in the underground has more to do with anonymity than economics. Many of the techniques described either create no billing record of toll calls, or they do so in a manner that eliminates the caller's association with the calls. COMSEC combines with rapid access to make phone service theft and fraud a viable option.

Phone service theft in the United States is quite common, and understanding the history and popularity of this activity will greatly enhance the underground communications plan. Obviously it is an inherently risky undertaking, and many covert ops would be best served

to completely avoid this option. Many of the techniques described can be integrated into the COMMO plan with no actual theft of service.

The following information is presented for information and academic purposes only, and is by no means an endorsement nor an approval of this activity by either the author or the publisher.

Placement of any foreign device on the commercial telephone circuit, fraudulent use of unauthorized telephone billing codes, and illegal theft of telephone service are felonies. The reader is advised to consider the legal ramifications and the aggressive prosecution history of this offense. Proceed at your own risk.

• • • • •

Documentary evidence of American citizens defeating the telephone billing process goes back at least fifty years. Few other cultures regard the intentional theft of service from a public utility as an acceptable form of behavior. In the United States, the "outlaw" mentality combined with the culturally characteristic lack of respect for authority is part of American folklore. In many respects, this uniquely American attitude is socially encouraged. Phone service theft is socially acceptable.

PHONE SERVICE THEFT IN THE 1950s

After World War II, Bell Telephone began to make note of college students using military surplus communications equipment to make free long-distance calls to home from campus. One notable technique employed an ordinary hand-crank field phone that was used by signal and artillery troops during the war to keep contact with command bunkers and foxholes. This large, battery-operated telephone generated an AC signal that electronically deceived the phone company's billing process.

College students in the early 1950s used this telephone to take advantage of an electrical characteristic of the phone company's newly installed *automatic message accounting* (AMA) system. When a long-distance call was made, the AMA system began the billing process only when the ring signal had stopped for three seconds. Normally the ring signal stopped when the phone was picked up at the other end, but the field phone put a signal on the line that made the AMA system believe that the phone was still ringing.

The phone company began making note of phone calls that apparently rang a distant number, sometimes for hours, for no explicable reason. Internal security personnel at Bell recognized that because the phone system ran on a circuit known as a *DC loop*, the theft technique being used was virtually impossible to defeat, although it could be detected.

Basically, when a phone rings, it is receiving a "ring" signal from the central office of about twenty pulses per second. When the person receiving the call picks up the phone, the DC loop circuit is closed, which tells the central office to stop the ringing pulse and begin the billing process. The modified field phone made the phone company circuitry believe that the loop had not been closed yet and thus the phone was still ringing. The slang term for the device was a *red box*, and it became popular on college campuses throughout the country in the 1960s.

PHONE SERVICE THEFT IN THE 1960s

In the 1960s many people began actively participating in antiestablishment behavior. College students and activists probably had the most significant impact on creating the notion that Bell Telephone was an evil monopoly worthy of creative attacks such as defeating the toll system to make free long-distance calls. Numerous underground and legitimate publishing houses put out

"guerrilla" manuals that covered a variety of techniques that were, in fact, quite effective in cheating Bell out of toll charges. (Many of these publications indicated that there was "poetic justice" in ripping off the telephone system while spreading the seeds of political discontent, since at that time Bell Laboratories was involved with research and development projects that were identified as contributing to the U.S. war effort in Southeast Asia.) Cheating the phone company became not only economically viable but a means of protest.

Activist Abbie Hoffman, in collaboration with Jerry Rubin and Ed Sanders, wrote a highly controversial guerrilla warfare manual entitled *Steal This Book*, which is representative of the literature prevalent during this era. In the book, Mr. Hoffman described a number of methods to make free telephone calls. He suggested, for instance, putting #10 washers in the coin slot in place of coins. He also described how to record the sound of coins dropping into the phone slot, and then play back the tape for the operator when she requested that coins be deposited to make a call.

Most notably, Hoffman provided a schematic diagram for a device known as a *blue box* that generated audio tones that affected the phone company's long-distance switching. When these tones were sent down the phone line, they essentially took over the circuitry at the local phone company switching center and permitted the user to make long-distance calls worldwide without any billing record ever being generated.

In its basic configuration, the blue box was simply a transistorized dual-tone oscillator circuit that produced a 2600 Hz (hertz) audio tone through a small speaker, which was placed over the mouthpiece of the telephone. The origins of the term "blue box" can be traced to a small plastic box sold by Radio Shack in which electronics hobbyists built their homemade circuits.

College students at MIT in the late 1960s are credited

with developing another device. Often referred to as a *black box*, it duplicated the tones generated at newer pay telephones as the coins were dropped into the slot. The students would play these tones over the phone line and convince the operator that they had actually deposited coins for a long-distance call.

Red, blue, and black boxes became a rage on campus during the counterculture era of the late 1960s. The political climate as well as the advent of semiconductor technologies made the miniature devices suitable for widespread use. Although a number of techniques were employed to attack the toll billing system, the general approach became universally known as *blue boxing* and was a very "in" thing to be able to accomplish. Indeed, the defeat of the telephone company was a technical challenge for the engineering student as well as a political statement for the liberal arts students.

One notable participant in the blue box phenomenon was a student by the name of Joseph Engressia. He was able to whistle a consistent 2600 Hz tone. In fact, his skill at whistling on this exact frequency was used by many electronics hobbyists to calibrate their homemade blue boxes. Engressia became known as "the Whistler" but he eventually was caught. The details of his case are somewhat clouded, but apparently he was arrested in Moscow after talking to a U.S. Marine guard at the American Embassy there. Alledgedly he openly discussed his theft techniques with many of the wrong people, possibly including Soviet officials. Engressia's arrest was well publicized. (After serving time in jail, Engressia cooperated with the phone company in developing strategies to halt the theft of phone service. He was hired as a "problem analyst" by Mountain Bell in 1977.)

Although Bell Telephone was aware of various theft practices that employed tone generation as early as 1961, their internal security apparatus concluded that the losses suffered through this somewhat simple technology

were not comparable to the amount of resources that would be required to halt the practice. This attitude changed very quickly.

By the late 1960s, service theft had become much more of a problem. The Hoffman book was widely read on campus, and the theft of service from pay phones became the first area of concern for the phone company. It developed a variety of electronic devices to defeat false indications of coin receipt. The technology race began.

As the phone company developed a strategy to defeat a specific technique, the students developed another method. Blue boxes became more reliable and smaller in size due to the development of transistor devices. The technical characteristics of the blue box were such that simple solutions to its use were not readily available. Once the box became palm size and portable, the tracing process became even more difficult to conduct.

Illegal pay-phone-to-pay-phone long-distance calls were made by many left wing radical groups in the late 1960s using well-calibrated transistorized blue boxes, and Abbie Hoffman's books, including *Steal This Book*, became best-sellers due to his high-profile activist role. (His works sold more than 3 million copies.) Eventually, Bell Telephone's internal security apparatus requested help from the federal government in dealing with this problem.

Organized Crime and Phone Service Theft

The fact that no billing record was generated with the blue box had significant appeal to organized crime elements who wished to place illegal bets and conduct transactions over the telephone that were untraceable. Due to the growth of the drug culture as well as new laws in 1968 regarding wiretapping (Public Law 90-351, 90th Congress, H.R. 5037, "Omnibus Crime Control and Safe Street Act of 1968," which placed strict limitations on government wiretaps), the illegal use of the telephone became the primary communications tool in the "underground economy" created in the 1960s.

The federal government responded to these activities by studying illegal communications techniques and using the "patterns" displayed by some criminal groups against them. An FBI undercover investigation in the late 1960s revealed that a group loosely associated with the Hell's Angels Motorcycle Club of California was using illegal pay-phone-to-pay-phone contacts to sell and distribute a home-made chemical stimulant known as methamphetamine. This group employed unauthorized third-party billing to make the calls from pay phone to pay phone, charging the calls to someone not actually involved.

These criminals utilized pay telephones in a manner that could be methodically tracked, since customers who were billed for the unauthorized calls eventually notified Bell. The FBI, in cooperation with the phone company, conducted a tedious and elaborate tracing program of pay phones being used illegally to call other pay phones using unauthorized billing. From this theft pattern, FBI investigators uncovered an elaborate nationwide organization. The stimulant was produced in clandestine labs on the West Coast by "cooks" who had a rudimentary knowledge of chemistry. The product was sold to distributors, who shipped quantities of it to large cities throughout the Midwest and East Coast. Methamphetamine became known as "crank" in street slang because it frequently was shipped inside the crankcase of Harley Davidson motorcycles.

This group had assumed that pay-phone-to-pay-phone calls were secure communications. The FBI exploited this primitive attempt at COMSEC and credits the group's clearly identifiable phone theft pattern (most of the calls were made from pay phones in bars frequented by bikers in the Midwest and along the East Coast) as helpful in the investigation.

By the early 1970s, the various techniques for toll cheating were well known among the counterculture and criminal fringe in the United States. AT&T was also

knowledgeable of the various techniques for service theft, and it began intense research projects to defeat the technology. The mainstream media also became more cognizant of the theft of phone service, and cases where AT&T prosecuted individuals caught stealing service were covered heavily in the press. This coverage actually caused the problem to become common knowledge among a wider segment of the public. Furthermore, the somewhat liberal media slant in the coverage of these cases made the thief appear to be a creative and clever individual and actually gave AT&T a somewhat negative image.

An interesting case that illustrates this socially encouraged "outlaw" mentality is that of John Draper. In the late 1960s, Draper discovered that, when blown into a phone's handset, a small plastic whistle given away as a prize in a popular breakfast cereal happened to generate the precise 2600 Hz tone oscillation that electronically seized an internal long-distance line from the phone company. Draper promoted his discovery, which functioned similar to the blue box, in a number of underground newspapers in the New York area. He was not aware that AT&T had begun electronic sensory development that detected this illegal tone.

Draper was caught and arrested, and his prosecution was covered in the national media. But instead of being identified as a criminal conspirator, Draper became known as "Cap'n Crunch," and his creative approach to phone theft was regarded as a prank against the monopoly of AT&T. The phone company suffered negative press for its prosecution of Draper, as well as some embarrassment, since a child's toy was used to defeat its internal toll billing process.

John Draper was convicted and sentenced to six months in jail. Yet he became an underground cult hero to a growing group of technical students and fringe groups who focused on attacking the telephone system's vulnerabilities.

PHONE SERVICE THEFT IN THE 1970s

Underground newsletters and publications relating to new alternative technologies, collectively termed *phone-phreaking,* reached their peak in the mid-1970s.

By 1974, AT&T had begun improving its switching systems. Low-cost microcomputer technology had been developed to allow high-speed electronic switching and automated toll-charge billing. This technology included special focus on internal security devices and systems. Known toll cheating procedures were considered in the hardware development.

The popular blue box became a foolish technique to employ. AT&T began an aggressive and successful campaign to detect and prosecute blue boxers. Users of the device who were caught were primarily businessmen and professionals. In fact, many well-publicized prosecutions were against wealthy and successful people.

On 27 March 1974, soul singer Ike Turner was arrested in California after his studio was raided by police. Pacific Bell Telephone had used its new sensory circuits to detect Turner's alleged theft of long-distance service. An illegal blue box was found connected to several lines in his recording studio. In order to build a criminal case against him, law-enforcement officials had also obtained a court-authorized wiretap clearance to record the conversations taking place. On 7 August 1974, the charges against Turner were dropped when the voiceprint evidence failed to show that his voice was actually on the recordings. One of Turner's associates was convicted and sentenced to six months in jail. He also had to pay about $3,000 in long-distance charges.

The cause of AT&T's poor public image in the 1970s was more than just a result of counterculture attacks and bad publicity. The federal government challenged and aggressively litigated AT&T's monopoly over telephone communications for most of the decade. As a result, this

huge corporation was split up into seven autonomous regional phone companies in the early 1980s.

PHONE SERVICE THEFT IN THE 1980s

One significant aspect of the company's "settlement" with the federal government suit was the introduction of a competitive long-distance service industry. Numerous small and large independent companies began to offer long-distance service to the public. In order to compete, these firms had to advertise substantial rate discounts compared to AT&T's long-distance toll charges.

Initially, these "alternative long-distance carriers" had to provide each customer a plastic card with an access number and fourteen-digit account number that the customer had to dial in order to save money on the call. Some people had to dial dozens of numbers accurately each time they wanted to use the discount long-distance service. This was complicated, confusing, and inconvenient for many Americans, so the concept of *equal access* was introduced. Now customers were allowed to select a specific long-distance company as their carrier, and no account numbers had to be dialed. By 1985, equal access was in place throughout most of the United States, but before that the plastic card with the long-distance access number was more common than a bank credit card in people's wallets, and a whole new means of telephone theft and fraud was born.

Phone customers who wished to make a long-distance call while traveling would give the operator their telephone credit card number or simply punch in the number when prompted to do so by the phone company computer. Criminals would observe this at a pay phone, make note of the number dialed, and then use the number or sell it at airports and bus terminals. Phone bills in excess of $100,000 arrived at people's doorsteps in large boxes from UPS because customers unwittingly let their numbers be

known. The customer was not actually charged for these illegal calls; the phone companies usually cancelled the card and wrote off the cost as a business expense. According to AT&T's annual report for 1982, it deducted more than $70 million in business expenses related to the theft and fraud of its long-distance services that year.

By 1984, telephone credit card theft and fraud had become a growth industry in the United States. Organized criminal groups and individuals worldwide actually made the theft and distribution of these account numbers a criminal specialty.

AT&T responded pragmatically with a research project developed by Bell Communications Research (BELCORE) to create strategies to deny physical access to a customer's billing number by unauthorized persons. BELCORE determined that there were a number of ways thieves were gaining access to the numbers, and it focused on the three primary causes: phone booth surveillance, sequential digital access by home computer, and mail theft.

All seven regional phone companies contributed to the cost of this project, and BELCORE developed the following strategies and technologies to attack the problem:

1. DIGITAL CARD READERS. These were pay phone-type terminals that had a slot on the side of the phone for customers to insert their long-distance credit cards. The units read the magnetic strips on the back of the cards to get the billing information. Customers did not have to read out the credit card number or enter it into the telephone keypad, where an experienced service thief could hear or observe the account number. These terminals were (and are still) successful in high-traffic high-risk locations like train stations and airports. The data card phone also denied the service thief use of any numbers he may have "collected" since there were no coin slots on the unit, and an actual card had to be inserted into the phone.

2. MULTINUMBER ACCOUNT SEQUENCE. When telephone credit cards were first issued, the first ten dig-

its of the fourteen-digit account number were usually the subscriber's area code and home phone number. A service thief could program a home computer with a modem to make a call through the carrier's billing system and sequentially attempt all possible four-digit access numbers until the billing computer accepted the entry. Although this required the thief's computer to attempt a possible total of 9,999 tries to gain access, it required no human participation whatsoever to conduct this mundane task. In fact, a typical home computer could make the connection every 5 seconds, or 12 times a minute, or 720 times every hour. Of course, if you attempt to guess a specific number out of a batch of 10,000 numbers, statistical probability alone would allow you to learn the number within the first 5,000 attempts. Since a personal computer could make about 17,280 attempts per day, it usually could come up with about three credit card account numbers every day for the service thief.

BELCORE recommended random fourteen-digit account numbers for each customer. A personal computer would not be able to statistically "guess" an accurate fourteen-digit number if it operated continuously for more than three years. BELCORE also developed software that would allow the billing computer to detect a large number of attempts at any code number, especially when these attempts were being sent by computer.

3. MAIL ACCOUNTING PROGRAMS. Many customers who had service initiated with a specific carrier received a telephone credit card in the mail. A common method of theft was to simply intercept this card in the mailbox. Before the customer knew the card had been stolen, thousands of dollars worth of long-distance bills would arrive.

BELCORE advised all carriers to send a follow-up piece of mail to each customer advising that the card had been sent and when. If customers failed to receive the card, they were asked to call a toll-free number to

advise the carrier, and the card would be cancelled. This simple approach was very successful and is now almost universally employed by all of the major long-distance carriers.

4. SECURITY SOFTWARE DEVELOPMENT. BELCORE provided software that allowed the billing computers to recognize "theft patterns" such as an inordinate number of calls being made on one account number. This information was electronically compared with the estimate of card usage given to the carrier by the subscriber when they applied for the account number. If the current usage drastically exceeded the estimate, the carrier called the subscriber and inquired about the call volume. If the calls were not authorized, the card was cancelled and the traffic analyzed in an attempt to catch the service thief.

Because long-distance service is a lucrative business that requires minimal labor intensive participation, a lot of small companies got into the long-distance game in the first half of the 1980s. Many of these firms did not fare as well against telephone credit card thieves and were forced to declare bankruptcy or merge with larger companies in order to stay afloat. Although telephone service fraud represents about 1 percent of total revenues for the industry as a whole, the losses some smaller companies were forced to face were too much. "Hostile takeovers" and acquisitions of the late 1980s also contributed to a thinning of the number of actual companies offering long-distance service. By 1988, U.S. Sprint, MCI, and AT&T had secured most of the long-distance market, with AT&T having the greatest percentage of customers.

The level of theft began to taper off in 1988 due to the efforts of an industry-sponsored organization known as the Communications Fraud Control Association (CFCA). This group began a multilevel campaign to attack the problem with the cooperation of most of the carriers as well as federal and state law enforcement agencies. The most significant elements of the CFCA program were its

aggressive prosecution of offenders and its antifraud education programs targeted towards population segments deemed most likely to defraud the phone companies: college students, military personnel, and prisoners. (These three demographic groups statistically represent more than one-third of the volume of telephone credit card theft and fraud in the United States as of March 1991.)

The CFCA also attacked the problem with an amnesty program. It compiled a detailed listing of credit card calls that were fraudulently placed from, for instance, a college campus. Then it notified all individuals who had enough prosecutable evidence against them that if they paid the toll charges, no criminal charges would be filed. In 1988, several hundred students at highly reputable American University in Washington, D.C., took advantage of this amnesty offer and agreed to pay MCI Communications more than $32,000 in unauthorized toll charges to avoid criminal prosecution. Also in 1988, more than one thousand underclassmen at North Texas State University agreed to pay MCI approximately $100,000 in a similar out-of-court "settlement."

As can be illustrated by the above historical overview, telephone service theft and fraud has been a problem for the communications industry for many years. The industry has been quite impressive at addressing virtually every technology and approach used to defeat the toll system. As service thieves developed strategies, the phone companies attacked each one creatively and in a pragmatic, effective style. Yet the problem is far from solved. In 1990, loss estimates from credit card theft alone were stated by the industry to exceed a half a billion dollars.

PHONE SERVICE THEFT IN THE 1990s

The 1990s are expected to see a resurgence of underground groups and extremist activity in the United States.

The means by which these groups are expected to communicate will be covered in detail in the next chapter.

Although the phone company has focused tremendous resources on a number of theft technologies, one basic approach is still virtually impossible to address effectively. The *parasitic interconnect*, or *intentional line seizure* as it is known in the telecommunications industry, exploits a universal aspect of the telephone circuit that cannot be corrected reliably. The service thief simply hooks into the phone line, either at the pole or at the outside terminal box on the residence, essentially installing his own extension on an existing telephone line.

Mail Order Companies and Phone Service Theft

This approach to ripping off the phone company has become a little known but active enterprise for a number of small mail order companies in the United States. Here is a sampling of advertisements from these firms:

BEAT THE SYSTEM. Never pay for the phone again! Free long-distance. This device tricks the phone. Money-back guarantee. For novelty purposes only.

PHONE COLOR BOXES. Designed by phone phreaks! Fifteen phone color boxes described. Dozens circuits; programs. Plus call forwarding conferencing; phreak history; fifty useful, simple and legal phone circuit plans.

BLACK MARKET. Hacking, phreaking, weapons, electronic surveillance communications, more. Hardware, software, plans, kits, books. $1.00 catalog.

Electronics, military, and do-it-yourself magazines carry these advertisements. Many of these firms have been around for decades. Generally, they provide plans for making your own blue box or similar device.

There are about two dozen firms in the United States that sell this type of information. It is generally true that companies selling the plans for blue boxes advise the reader of the risks as well as limit their own liability by stating that the product is for "information purposes only."

The fundamental problem with these companies is that they are selling technology and techniques that are easy for the phone company to detect. Although there are parts of the country where a blue box will still work with only a slight chance of detection, the fact is that the technology is extremely dated. This is seldom stated in their offerings. The individuals selling the information are after the novice in the phone theft game.

An example of line-seizure technology available by mail order is a basic telephone set with alligator clips connected to a wire. Called the "Adventurer's Telephone Set," it is sold for about $100 and basically is a copy of a telephone wireman's set for use along the telephone line. This simple device has made its way into criminal hands and the inventories of a number of terrorist groups.

For example, on 18 October 1984, the FBI raided a home near Sandpoint, Idaho. The residence, located about fifty miles from the Canadian border, had been occupied by Gary Yarbrough, a member of the violent white supremacist group known as the Order. Yarbrough barely escaped that evening, but in the attic of the home was found a number of weapons (including the suppressed .45-caliber MAC 10 submachine gun used to kill Alan Berg, a Denver, Colorado, radio talk show host), hundreds of documents, and a telephone lineman's set that he had used to make illegal telephone calls to other members of his group by hooking into phone circuits in rural Idaho and Washington. Court testimony revealed that a number of the members of this domestic terrorist group had employed intentional line seizure as part of their communications plan.

Other groups outline phone service theft and line-seizure techniques in their training manuals. The book *EcoDefense: A Field Guide to Monkey Wrenching* by Dave Foreman, the leader of the group Earth First!, is a recent example. On page 228 of the second edition of this best-selling book, the author recommends line seizure at a

business or apartment location. He describes in simple and accurate terms how to connect a telephone or computer modem to a telephone line as a means of anonymous computer hacking. He further advises placing security elements to observe the business or residence while theft of service is occurring. Foreman states that line seizure is useful in computer sabotage because authorities will attempt to trace the call, and if the trace is to an anonymous business, the hacker can get away.

In his book *On the Run,* CIA defector Philip Agee described his approach to phone service theft while he was hiding from the Agency in France. Agee states that he often used a certain pay telephone that was modified by French students to make free calls. A pin was inserted at the toll counter to stop it from advancing. He also described using a certain professor's telephone line to make international calls by seizing the line when it was left unattended at night.

Line seizure is the simplest and quickest means of initiating an illegal phone call, although it is certainly not the safest way to go. The fact is that a record of an unauthorized call is created, and it is very likely going to be disputed by the legitimate subscriber. This is important to consider, since the point of covert communications is to avoid calling attention to oneself. Yet in general, line seizure is prevalent because it is simple and it works, and therefore, it is the most common means of service theft by underground and criminal groups.

Computer Technology and Phone Theft

Technologies recently developed to obtain credit card account numbers on a large scale focus on illegal computer access. *Computer hacking* has developed into a major threat to a number of business and government data-base systems. The penetrations conducted in the last few years have been more harmful and malicious than those conducted in the early 1980s.

The home computer has been the foundation of a new counterculture of technical students and software development hobbyists. These loosely organized groups tend to practice their skills on supposedly secure targets. Some groups specialize in creating mass programming errors in the target system. These errors cause losses of data and files and are termed *viruses, bugs,* or *worms,* depending on the programming sequence employed to attack the system. An inexpensive home computer and a modem connected to a telephone line seem to present a number of temptations to the computer hacker.

Some hackers specialize in obtaining confidential or internal information files from large companies and government agencies. The long-distance credit card thief has focused on this activity. The hacker gains computer access to a long-distance carrier's internal billing system and illegally obtains bulk amounts of telephone account codes.

As in the 1970s, media coverage of these illegal computer penetrations tends to focus on the creativity and "prankster" image of the hacker. The commercial or government networks that are the victims of the illegal access usually are not given any amount of sympathy. News reports covering these cases frequently regard them as amusing "adventures" of "spirited" students.

Just as the telephone company retained blue boxer John Draper for security development in the 1970s, many companies today are hiring successful computer hackers to assist them in developing countermeasures to illegal system access. Many successful and prominent computer industry figures have openly admitted to a number of hacking enterprises in their college years. Stephen Jobs, founder of Apple Computer and now president of NeXT Computer, admits to having "dabbled" in blue boxing and other phone service theft techniques while in college, according to interviews and reports.

The typical young computer hacker seldom gets involved with large-scale criminal activities. Unfor-

tunately, the computer has become a tool for a number of organized crime groups in conducting their illegal activities. Telephone credit card theft is a lucrative industry in the United States, and the personal computer has become an effective tool in gaining access to a large amount of active account numbers, which are sold and distributed nationwide. Often they are sold at major air terminals and bus stations to travelers as a means of calling relatives and friends at a flat rate. (In New York City, the going rate for this exchange is $3.00 for a call anywhere in the United States and $5.00 for a call anywhere in the world.)

The problem of computerized theft of account numbers on a large scale has been addressed by most of the major long-distance carriers. On 8 May 1990, agents with the FBI and Secret Service began a sweep of arrests after an eighteen-month investigation into a group of hackers who stole phone billing account numbers. During simultaneous raids in fourteen U.S. cities, agents seized 40 personal computers, 23,000 disks, and other materials. Five young men, ages 19 to 24, were arrested. Among other charges, they were indicted for theft of long-distance toll services in excess of *$50 million*. According to a spokesman for the U.S. attorney's office in Phoenix, Arizona, where the investigation was based, the arrests were "just the tip of the iceberg" in terms of organized computer theft of telephone billing account numbers in the United States.

• • • • •

The basic premise of outlining the history of phone service theft is for the reader to understand that to steal phone service as a part of any communications plan is not a new or particularly original approach to covert or underground message exchanges. This overview should provide insight into the tactics and technologies that have been employed, as well as give the reader a clear understanding of the inherent risks involved.

10 ● COMMERCIAL CIRCUIT ACCESS STRATEGIES

This chapter will focus on the tactics and technologies employed by professional thieves, criminal elements, and computer hackers to defeat the telephone toll billing process to the tune of more than $500 million a year.

The operative is advised to review and assess the inherent risks of each of these strategies individually before making the decision to execute any one approach.

It is important that the reader understand that this very illegal activity involves electronically attacking an extremely alert and sophisticated communications system that is technically proficient at catching unprofitable, unauthorized penetrations. Therefore, conduct these maneuvers at your own risk. If you believe you are clever enough to continuously commit a felony against a large corporation with aggressive internal detection and investigative assets, you may learn otherwise at your own expense. This information is for academic purposes only.

• • • • •

Essentially, there are three approaches to attacking the security of the TELCO circuit for electronic access and illegal service connection. All of these strategies are designed to function within the alert sensory environ-

ment of the modern phone system. This circuit is a complex electronic "organism" that has built-in computer protection from intrusion. In fact, the system is designed to detect, locate, and attack a penetration in a manner much like a living organism would attempt to deal with a germ or a virus. It also continuously learns, develops, and "mutates" to compensate for new intrusion strategies as they develop and are identified by the flexible system software and detection architecture. Understanding the above analogy is important if you wish to operate electronically within this hostile sensory environment.

The three most useful penetration strategies are:

1. PARASITIC INTERCONNECT. This broadly defines the introduction of specialized hardware to illegally function somewhere within the circuit. Network interface cable rerouting, covert "insulation displacement," and inductive collection devices at the multiplex terminal are all examples. This technique is also termed *intentional line seizure* by the phone companies.

2. ACCESS CODE INTERCEPT. This approach includes passive and active measures used to gather bulk amounts of functional access codes. Internal phone company authorization codes and active subscriber account numbers are collected electronically using a variety of technologies.

3. SYSTEMATIC DECEPTION. This is the most advanced approach currently being employed. It is a difficult-to-detect "front door" strategy that employs the human elements of the system for access. The approach gives the indication of a legitimate service request by a potential subscriber and requires the creation of a detailed "electronic identity" that will meet the phone company's credit profile. Once initial low-level access is gained with this nonexistent "customer," the authorization code is electronically injected into other systems and a stream of seemingly legitimate access codes are provided unwittingly by the service request operators. One sig-

nificant aspect of this approach is that even when detected, it is handled as a standard uncollectible account and not as an actual theft.

Each of these approaches has technical merit, but before deciding to execute any one procedure, the reader is advised to examine all the strategies discussed. Each approach is designed to attack specific vulnerabilities of the telephone system circuit. In keeping with the original analogy of the telephone system being a complex "electronic organism," these strategies seem to work because they cause a mild, noncontagious "infection" for which the system is incapable of producing an "antidote" or software "inoculation." Each access acquisition strategy must, in fact, be somewhat "acceptable" to the system and employed only to a certain tolerance envelope that essentially is unknown by the intruder. The success of these approaches is probably temporary due to the system's constant growth. Intensive usage of any one technique will accelerate detection and actually assist the system's security analysts in developing effective countermeasures.

PARASITIC INTERCONNECT

This strategy is the easiest and fastest method of circuit penetration. Using easily modified hardware, the operative covertly installs a secondary extension into the system from an access point that is selected on the basis of security and function. The two objectives that can be realized from this method are:

1. INSTANT CONNECTION. The circuit can be entered, the legitimate subscriber can be bypassed temporarily, and calls can be made quickly on an as-needed basis.

2. CODE NUMBER COLLECTION. A parasitic interconnect can be executed on a strategically located pay telephone or even a "credit card only" terminal to gather a large number of access codes. The goal is to record and

collect the digital tone code sequences as they are entered by the subscriber.

Speed and simplicity are characteristic features of parasitic interconnect. When executed randomly and carefully, this strategy exploits a vulnerability of the system that is, for all practical purposes, impossible for the phone company to correct or defeat.

Parasitic interconnect is technically possible due to the breakup of AT&T (Bell). The commercial market now has thousands of private companies that work in and around the telephone circuitry—installing hardware, troubleshooting line installations, and so on. While in the 1960s and 1970s Bell Telephone had internal detection equipment to learn if someone had placed an extension or any other foreign device on the telephone circuit, today consumers are permitted to do so, and a number of companies offer services that involve the physical access of the circuit.

Many small residential and commercial prewiring firms employ former telephone company technicians to perform installations. It is not uncommon to see an individual with a telephone handset and a tool belt at a terminal box or wiring junction testing equipment or lines. Yet this person is not necessarily a TELCO employee. This operational characteristic of the modern telephone circuit is perhaps one of the most useful vulnerabilities that can be exploited in access acquisition.

The telephone system is not as complex as it appears. There are a number of access points at which the operative can safely install a parasitic device, and as long as the risks and inherent dangers are considered in operational planning, the use of the parasitic interconnect technique can be a flexible component of an underground communications plan.

Risk Assessment

A parasitic interconnect is installed on the circuit in

the same manner and using similar equipment as an illegal wiretap. Consequently, there are some risks involved with the execution of this approach. If the connection has subscriber-installed detection equipment on the line, the parasitic device will be detected immediately and the subscriber will be alerted. Precautionary measures are described later to protect the operative from this rare but potentially compromising condition.

The parasitic interconnect can also be detected easily by the random phone company technician who happens to be servicing that specific location for any number of reasons. The presence of the parasitic device will be recognized as either a service theft or possibly an illegal wiretap. Either way, the operative will be at risk of compromise.

These two operational threats must be neutralized somehow. In most cases this is not completely possible. There are techniques and hardware that can assist in this area, but the first thing the operative must understand before employing parasitic interconnect is basic telephone system wiring practices.

Structural Overview of the Telephone System

At the end of the telephone system circuit there is always a telephone that must be bypassed temporarily to avoid compromise from either end of the circuit. There are a number of suitable entry points in the wiring configuration at which to do so. Selection of the most secure access point in any given situation is based on understanding the general characteristics of the system.

By the early 1970s, AT&T had more than 100 million telephones installed. The complex system of networks designed to allow any one telephone to contact another can be divided into three basic types: Long Haul Network, Exchange Area Network, and Local Network. This system now connects 570 million phones worldwide.

The *Long Haul Network* uses satellite ground stations as well as microwave and fiber optic links to transfer

large numbers of conversations worldwide along "trunks." (A trunk is simply a circuit linking two switching center systems.) Fiber optics technology is proving extremely useful in this area. One glass fiber as thin as a human hair can carry thousands of voice channels. A standard AT&T FT4 fiber optic cable carries 4,032 channels simultaneously. The major competitors in the long-distance industry have independent Long Haul Networks. MCI (Microwave Communications Inc.) uses microwave links for its service, but U.S. Sprint has invested heavily in fiber optic links.

The *Exchange Area Network* is the intermediate link between the Long Haul and Local Area Networks. The Exchange Area is focused on local inner city switching and linking the subscriber to toll services. It typically is confined to those areas that the subscriber can call at no toll charge, termed the *local calling area*. The Exchange Area Network employs wire, microwave, and fiber optics to link each central office to the other and itself to the Long Haul Network.

The *Local Network* is the wire system that connects an individual subscriber's phone to the rest of the system. The Local Network is confined to the *central office* (CO) and the thousands of wire *pairs* (the two wires running to the residence) that connect throughout any specific geographic area. The central office is identified by the first three digits in a phone number, or the *exchange number*. An understanding of the wiring characteristics of the Local Network can greatly enhance the employment of parasitic interconnects within the system.

The "typical" central office is difficult to define. It may cover several square miles or be confined to a few blocks. It may actually be nothing more than a *remote switching unit* (RSU) containing computer circuits to route each call. The average central office wire center in an urban American city covers about 12 square miles, about 150 square miles in a rural area.

Running from the central office is a large number of cables known as a *feeder network*. These cables generally are underground and cover a specific geographic area known as the *feeder route boundary*. The local distribution area for a central office feeder network is divided into several *serving areas* where cables come up from the underground routing conduit to an interface box. (The serving area can be several city blocks in size.) The network now travels aboveground, typically on telephone poles containing several hundred or thousand telephone pair cables. These thick pair cables are routed to individual blocks, where they get progressively smaller in size as individual pairs connect to homes. By the time the cable reaches a specific street corner it is usually a 50-pair cable.

Parasitic Interconnect Access Points along the Telephone Circuit

Terminal wiring points are those portions of the telephone company circuit that terminate at the subscriber location. These points can be divided into two basic areas: those access points that are the property and maintenance responsibility of the phone company, and those that are the property of the subscriber.

Essentially there are ten usable access points along this circuit, each of which will be covered in the following pages. The technical descriptions and characteristics and the risks and benefits of each point will be compared and assessed. With care, parasitic devices can be employed at any of these points, and the target traffic can be collected safely if the precautions explained in the text are considered and adhered to.

The following are the parasitic device access points on telephone company property:

1. Telephone pair cable.
2. Telephone pole.
3. Terminal box.
4. Drop wire.

5. Network interface.

The following are the parasitic device access points on the subscriber's property:

1. Interface to junction wire.
2. Wire junction box.
3. Station wire.
4. Modular phone jack.
5. Telephone wire and unit.

Telephone Pole

Although underground wiring is slowly replacing the telephone pole in modern metropolitan areas and suburbs, the telephone pole usually is the starting point at which the operative can access a specific subscriber line. A standard telephone pole is creosote-treated hardwood standing 18 to 20 feet high. The pole may also carry high-voltage power lines, cable TV routing lines, and traffic-light control boxes. Caution should be used in attempting to access a phone line via the pole—it is the most dangerous and high-profile access point.

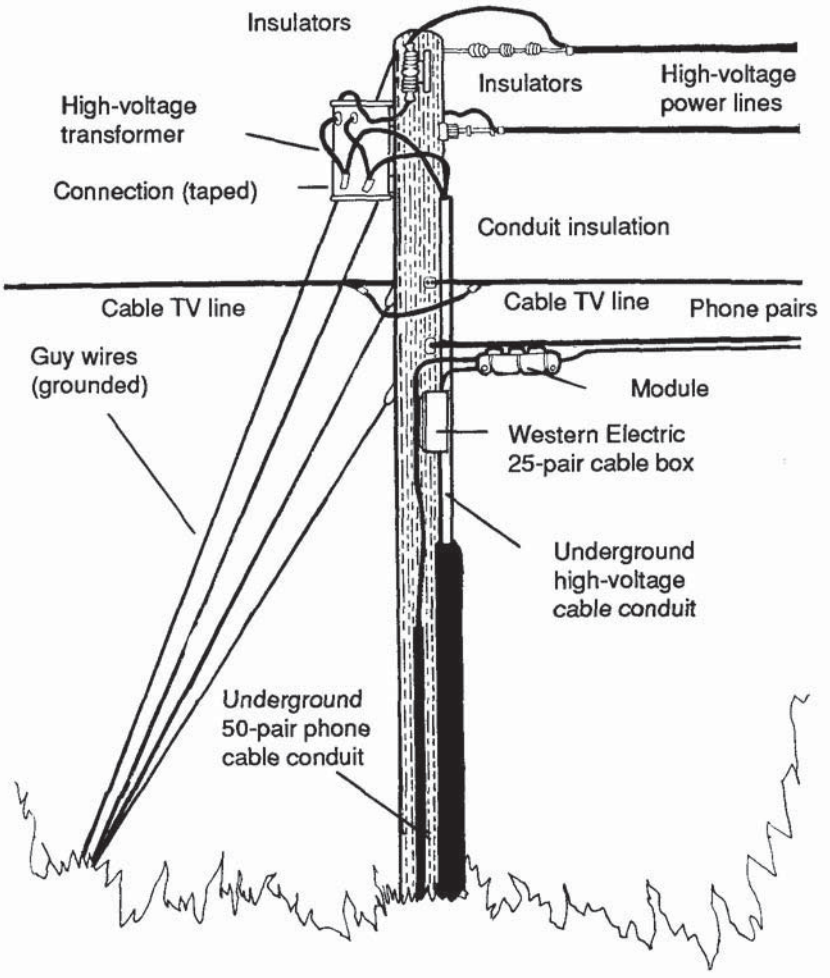
Telephone pole climbing requires metal spikes that are attached to the lower legs with leather straps. These spikes are termed *gaffers* and require a bit of practice to use safely. Gaffers can be purchased at surplus stores, hunting supply stores, or sporting goods outlets, as they are used by some hunters to climb tall trees and install metal seats known as "deer stands." A safety harness is also required.

Covert pole climbing usually is done late at night. Some important points to remember about pole climbing:

1. Wear durable gloves and boots and loose-fitting clothes that have no tears or layers that may get snagged or impede the climb. Obviously, dark colors should be worn.

2. Keep the gaffers clean and sharp. As you climb, gaff the pole about 1/4-inch deep and climb in 8- to 12-inch steps. Take your time, planning two or three steps ahead.

3. Never climb alone. Have an observer to keep an eye



This is an underground installation where high-voltage, phone, and cable TV lines share the telephone pole. To access the terminal box, the operative must climb around the deadly high-voltage conduit. Do not climb these types of poles.

on the area while "spotting" for you. This protects you from the risk of being caught and also provides a safe extraction and first aid source should you get injured during the climb. Always wear a safety harness when climbing.

Mounted directly on the telephone pole is an aluminum box known as a *terminal box.* Inside the hinged door is a series of connecting terminals, usually from six to twenty-six pairs of screw or nut-type points. This is where the subscriber lines emerge from the cable.

From the terminal box there is sometimes a long metal cable guide on the telephone wire. This is a terminating housing that allows the 25-pair telephone cable to be interconnected to the terminal box. Sometimes there is no terminal box, just this long housing directly on the thick 25-pair telephone cable, about 2 to 4 feet from the telephone pole.

From either the 25-pair cable guide or the terminal box there is a thick pair of black wires that connect to the residence. This line is known as the *drop wire,* and it is where the operative hooks up the parasitic interconnect device. The drop wire can be traced from the inside of the terminal box, and the device can be hooked up on the target line.

There are some safety precautions that must be observed for any hookup at the telephone pole. If you are touching these terminals when the phone line is receiving a ring signal from the central office, you will receive a substantial electric shock of about 96 volts. Although this voltage surge is not dangerous or even lethal, when you are on a pole in the middle of the night with sweaty palms, the jolt may cause you to pull away from the pole, loose your foothold, and fall to the ground. This has been known to happen to inexperienced linemen.

Pole climbing requires a substantial amount of practical experience to be safe and quick. It is recommended that you assemble your equipment and practice on a remote pole. The pole does not necessarily require a terminal box—simply practice careful climbs up and down

the pole, stopping occasionally and working on a mock terminal box.

Once daylight practice is comfortable and safety becomes a habit, practice in low light such as dawn or dusk, and then graduate to complete darkness. It is an indescribable experience to be up on a wooden pole in complete darkness, even without the adrenalin rush of possible detection and compromise. Without practice, therefore, the operative will find himself extremely distracted and unable to perform a simple parasitic hookup.

Many telephone poles have L-shaped ladder spikes every couple of feet. They can be accessed from the ground by climbing the pole up to the first rung. These ladders make the climb much safer; however, a safety harness should *always* be worn, regardless of the presence of these rungs.

Although climbing up a pole by shimmying a few feet to the ladder rungs is relatively easy, the operative should *never* attempt to climb a ladderless pole without gaffers. This is much more dangerous than it appears. The climb up seems quite easy, but after clinging to the pole for a few minutes with just your legs and the harness while you work on the terminal box, your leg muscles will begin to constrict. When you loosen your hold to descend down the pole, your muscle control will be affected and you very likely will fall.

Never climb a pole that has high voltage lines. Never climb a pole during high winds or any amount of rain. Make note of whether there are trees close by the pole that may obstruct your climb or work. Also make note of possible stinging insect nests on the pole or in a nearby tree. At night, bees and hornets are dormant to a degree, but your intrusion will be unwelcome.

Careful premission planning, good equipment and safety habits, and an alert spotter are all key to quick, efficient late-night pole climbing. With practice, the entire maneuver can be executed in four to six minutes.

Terminal Box

The terminal box is where the operative can hook up on any pair of lines and make calls using a business or residential line. One of these types of terminals can be found near most every dwelling in the country. Loosen the terminal box cover, place alligator clips on any pair, and run station wire down the pole to your phone. If you performed the maneuver correctly you will get a dial tone. You can place calls from a vehicle parked next to the pole, or you can hook up a modified cordless phone right at the terminal box and talk from blocks down the street. When you are finished, retrieve the wire or the phone unit quickly and clear the area.

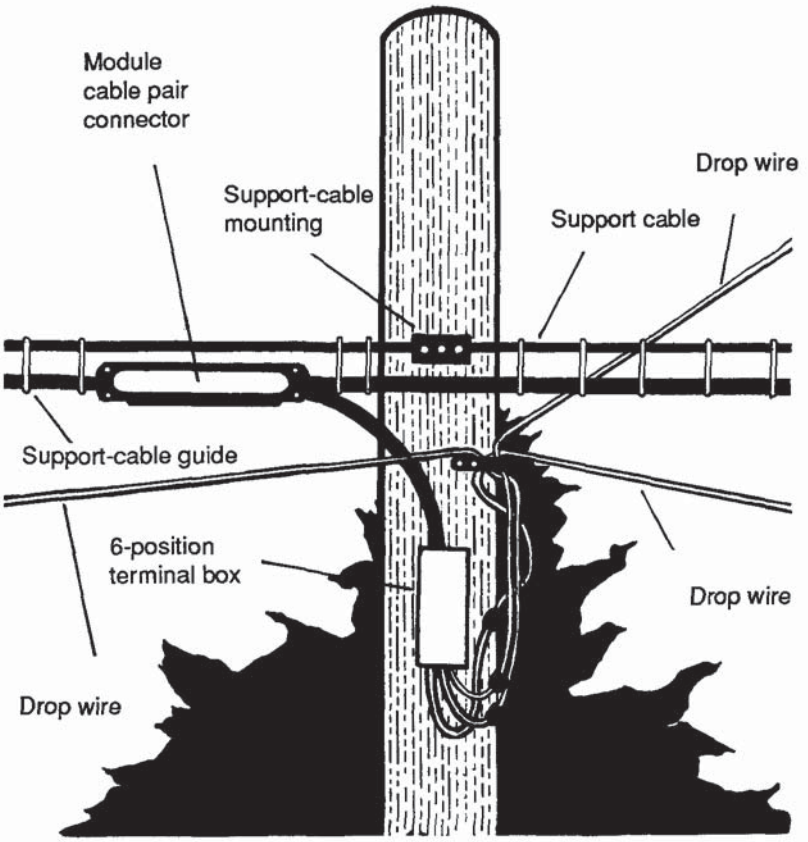
WARNING: The telephone pole is a dangerous access point. The illustration on page 157 shows one with a terminal box and cable as well as other wiring. Note that on top of the pole there are a transformer and high-voltage lines, which feed up from an underground conduit run. This configuration can be found at many locations that have underground wiring. In order to access the terminal box, you have to climb directly over this conduit run.

Never attempt access at this type of pole. If you accidentally touch the wrong wire or if your gaffers accidentally pierce the high-voltage conduit on the side of the pole, you will be electrocuted and die. The voltage and current at this type of pole are so intense that you will stay connected to the wires while being electrocuted. If your observer tries to assist, he or she will also be electrocuted. There are enough access points in any given area that you do not need to climb a pole that has high-power wires attached. This is extremely dangerous and should always be avoided.

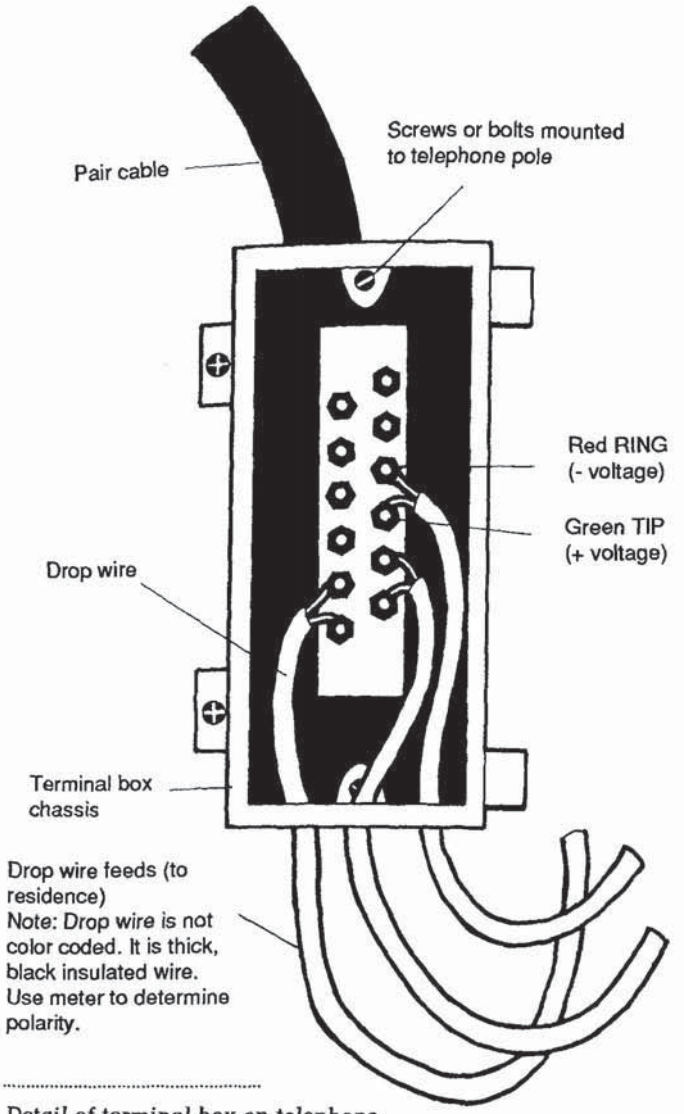
Terminal boxes come in a variety of sizes. Most are aluminum and rectangular in shape and are slate grey or flat black in color. They may have sliding or hinged doors to allow access to the terminals. The box can be easily distinguished on the telephone pole; it is where the drop

wire pair feeds to the subscriber building. Newer terminal boxes can be found right on the telephone pair cable. These boxes are long, narrow units generally located a foot or two from the pole.

Only common tools are required for access and hookup to a terminal box. If the box has a screw-type interlock on its doors, a flat-tip screwdriver will be needed (this is seldom encountered, but when it is, it can be observed from



Close-up of top of telephone pole showing terminal box.


Pair cable
Screws or bolts mounted to telephone pole
Red RING (- voltage)
Green TIP (+ voltage)
Drop wire
Terminal box chassis
Drop wire feeds (to residence)
Note: Drop wire is not color coded. It is thick, black insulated wire. Use meter to determine polarity.

Detail of terminal box on telephone pole with cover removed.

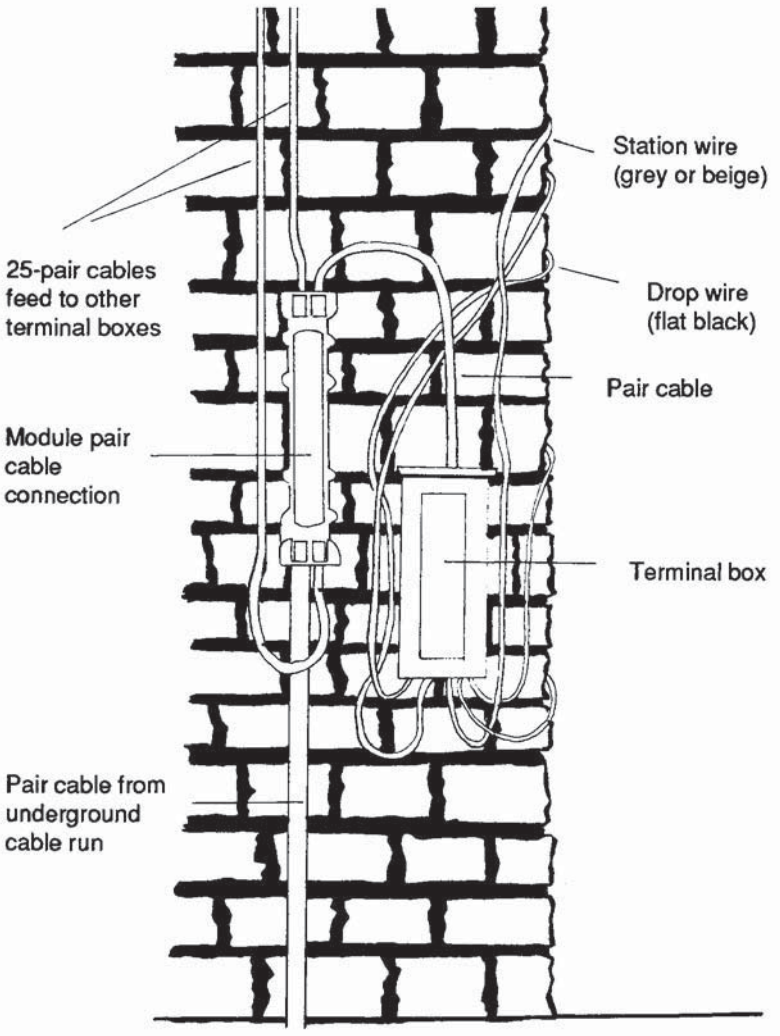
the ground and planned for). An insulated pair of pliers is helpful if the operative wishes to hardwire the parasitic device directly to the terminal, though regular-size alligator clips usually are better for the hookup.

A pencil eraser is handy if there is a lot of corrosion or oxidation on the copper or brass terminals—a better electrical connection can be made if the terminals are cleaned by rubbing the eraser vigorously at the contact points. A small penlight with a red filter is also recommended. (The red filter provides ample illumination with less impact on the operative's night vision, which will be needed for the climb down the pole.) It should be operable with one hand and have a pocket clip for quick access.

If any problems are encountered in the functioning of the parasitic device, a small analog voltmeter with probes is handy for continuity and voltage checks. Rubber insulated dishwashing gloves provide a good degree of hand protection and a level of insulation when handling the lines. These gloves also eliminate fingerprints much better than surgical gloves. A more detailed overview of circuit handling tools and techniques will be covered later in the chapter.

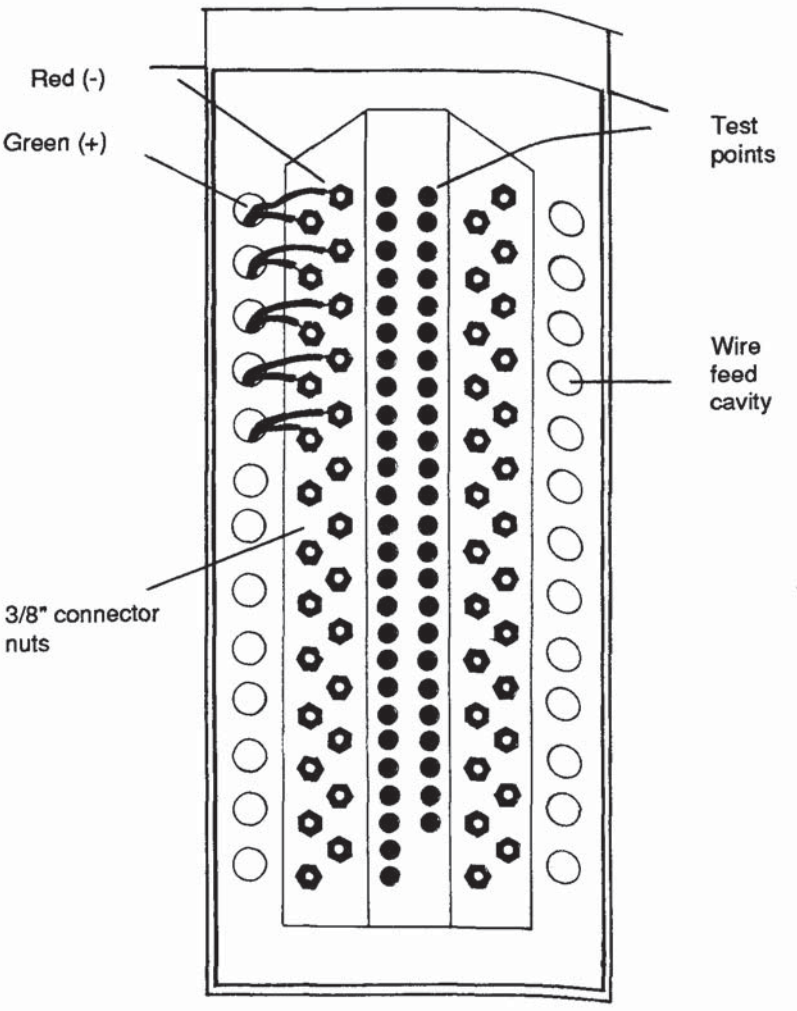
The terminal box can be used to place surveillance devices on a line or seize a specific circuit. The terminal box most encountered in the United States is the Western Electric model NH 25. This connects directly to a standard 25-pair cable group to provide up to twenty-five lines in a given area. The NH 25 has no lock or hasping device; you simply pull down on the top of the faceplate and the terminal box opens by a hinged door.

Terminal boxes do not have to be on a telephone pole. As shown in the illustration on page 164, the box can be mounted on a brick wall outside a building, a common installation found in alleys in most cities. Note that there are five lines connected to this box. The illustration on page 165 shows the internal wiring of this Western Electric NH 25 terminal box.



A terminal box on the side of a building, common in city alleys. It is an excellent location for line seizure ops.

This would be an ideal access target. The box in the illustration provides service to small-business subscribers in a downtown building. In order to make free calls, sim-



Detail of terminal box on building wall with cover removed.

ply open the box and hook up to the target terminal. If you do it late at night when the business is closed, no one will detect your illegal usage until the phone bill comes. In

order to defeat customer-installed detection equipment, simply disconnect their service by removing one of their wires before you hook up your parasitic device.

The subscriber line is secured to the terminals with a 3/8-inch nut and threaded screw assembly. Use a nut driver or a pair of pliers to remove one or both connections from the terminal box, then hook up the phone device at these terminals. This bypass denies anyone access to the line you are using.

In order to deal with the risk of compromise, you also should have a means of detecting someone picking up a phone on the line you are using. When you perform a bypass to seize a circuit, the person who actually owns the phone will get nothing in the earpiece if they pick it up. They may assume the line is dead. A simple means for the operative to know if someone has attempted to use the line is the *ohmmeter.*

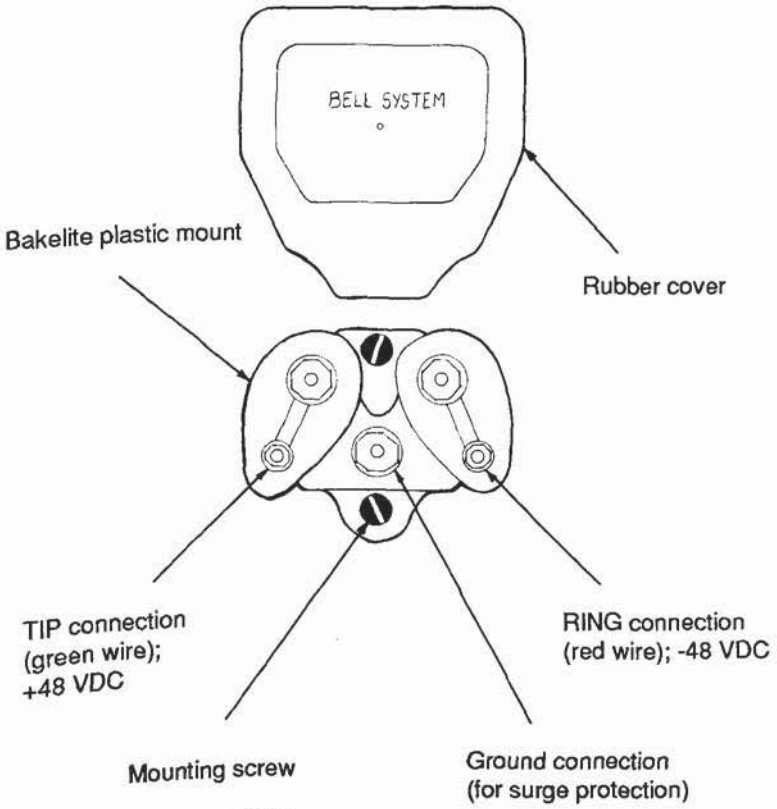
Bypass the circuit by disconnecting the subscriber from the line at the terminal box connection. Place an ohmmeter on the drop wire going to the subscriber phone. When the phone is on the hook, it will give a reading of more than 1 million (meg) ohms. If the subscriber picks up the phone, the meter will immediately register a drop in resistance to around 20,000 ohms. If this occurs, disconnect your call quickly. When the meter reads above 1 meg ohms again, the customer has hung up the telephone. Quickly reconnect the drop wire to the terminal box. When the customer goes to pick up the phone again, he will get dial tone as normal. (This problem is covered in more detail later in this chapter. A simple circuit is described that will give the operative a visual or audible indicator that the line is in use.)

Network Interface

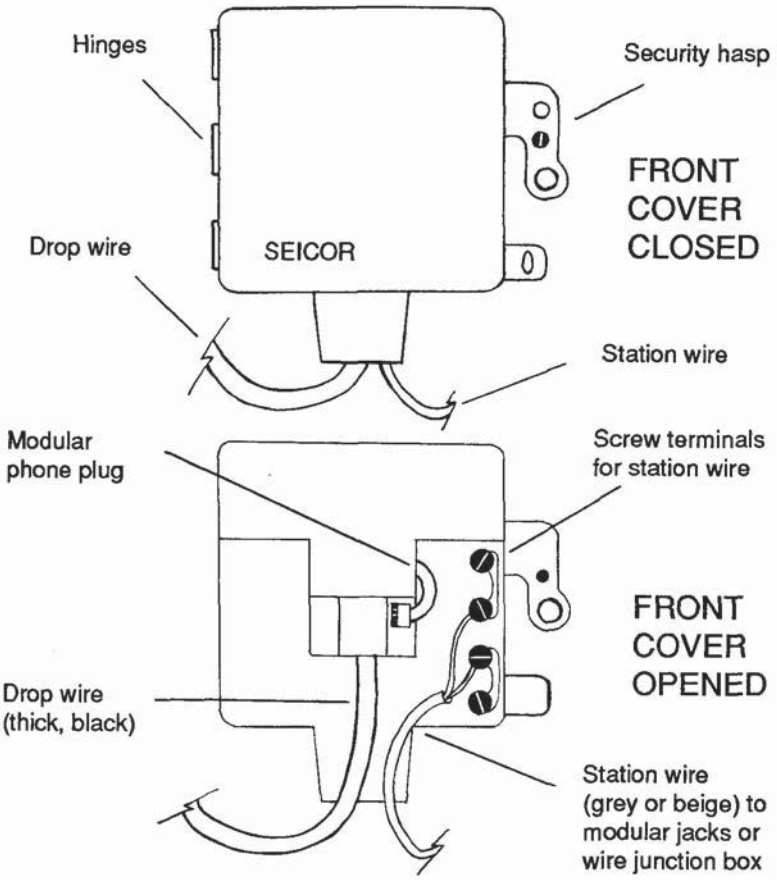
From the terminal box on the telephone pole, the drop wire goes to a small connecting block on the side of the building close to ground level known as the *network*

interface. If it is an older home or a trailer or mobile home, it may be right on the pole next to the dwelling. Sometimes there is a surge protector between the drop wire and the network interface.

Different types of terminals serve as the network interface in a typical telephone system. Older models are simply a Bakelite plastic box with two terminals inside of a rubber housing, as in the illustration below. Newer plastic models are square covered units (page 168).



Old-style network interface common on older buildings, in rural areas, and in mobile home parks, where it may be installed directly on the pole.

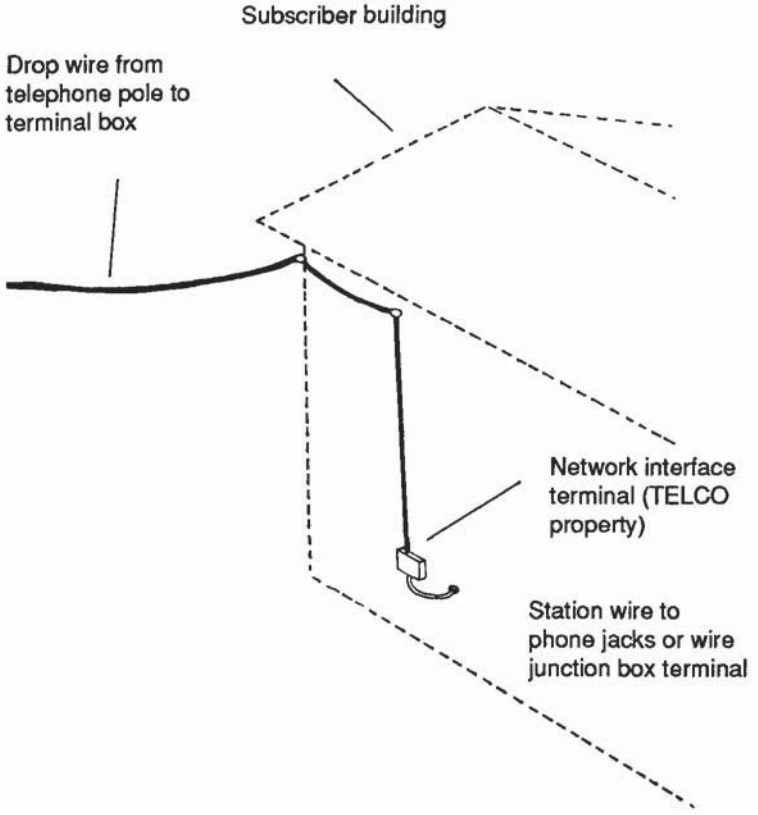


Modern network interface.

Since the breakup of AT&T, the various phone companies only have control of and access to the subscriber's phone circuit up to the network interface. In phone company terminology, this is known as the *point of demarcation,* since everything beyond this point is the customer's responsibility to maintain and service. The phone companies generally offer a complete service plan to maintain both sides of the system, but the customer has the

option of hooking up extensions and peripheral devices at his discretion and risk. If the circuit is damaged on the subscriber's side of the network interface, he must contact the phone company or an outside technician to repair it at his own expense.

The advantage of installing a parasitic device on the subscriber side of the point of demarcation is that the phone company is unlikely to detect or observe the physical installation of the device because it is not in their area of responsibility. The access point where the phone com-


Subscriber building
Drop wire from telephone pole to terminal box
Network interface terminal (TELCO property)
Station wire to phone jacks or wire junction box terminal

Network interface location on subscriber's house.

pany is no longer concerned can be as little as a couple of feet from the interface box. Also, since the subscriber may have any number of devices on each line (answering machines, computers, fax machines, etc.), the typical voltage drop on the line caused by the parasitic device is of no consequence to the phone company's central office. (Before the breakup of AT&T, the presence of any device that lowered the voltage on a line alerted the phone company that the subscriber had installed an illegal extension phone, which at the time was an extra charge.)

As an access point, the network interface is probably the ideal location for parasitic interconnect. It is usually outdoors, where cover of darkness will allow quick access and hookup. It does involve risk, however, because the unit is close to the subscriber building, and anyone near the building late at night will be suspicious.

Accessing the wiring of the network interface depends on the type of model it is. The illustration on page 168 shows a 1990 model SIECOR network interface. This weatherproof grey plastic enclosure has a screw hasp on the hinged door. It also has facilities for a padlock to discourage access at this point. Although the padlocked door is relatively secure, the hinges can be removed quite easily and then replaced once access is gained. (It is a relatively new industry specification to have physical security devices such as locks at the network interface point, though this trend is likely to continue as the system is upgraded. The physical security of terminal boxes and network interface enclosures is to protect against service theft and illegal wiretaps.)

The network interface typically encountered at a residential subscriber setup is difficult to describe. The unit may be decades old and heavily corroded, or it may be brand new and secured inside the building. Visually trace the drop wire from the pole to the building. It generally has a tension cable to secure it and feed it down the outside wall of the building, where it either terminates at the

network interface box or feeds directly into the lower floor or basement, where the box is located.

Wire Junction Box

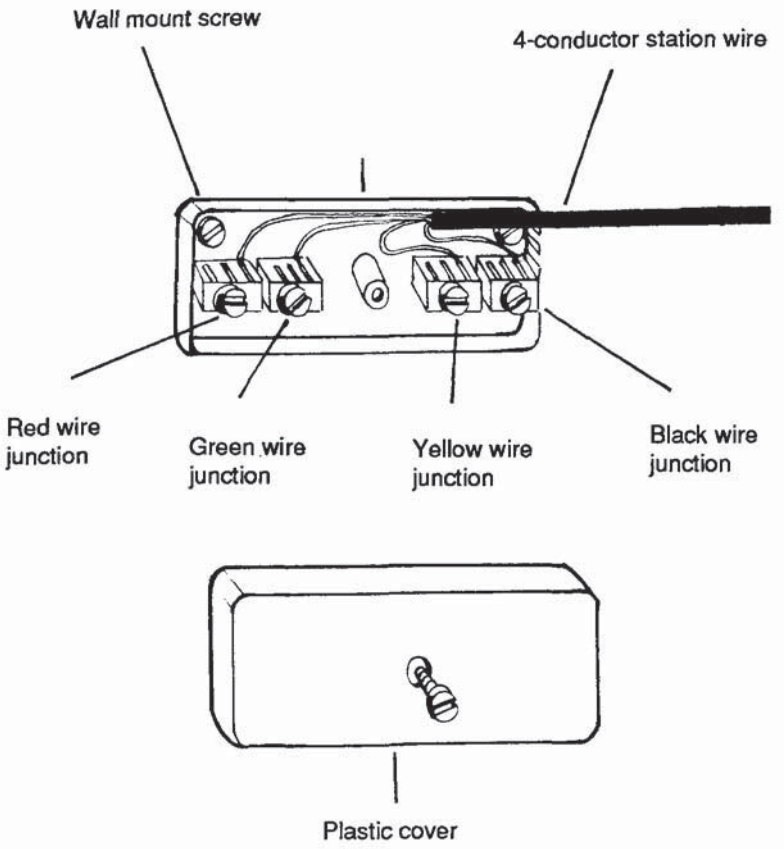
From the network interface there simply may be grey *station wire* running directly to the modular phone jacks installed in the residence. More typically there is another terminal box known as the *wire junction box.* This is the interconnecting block between the network interface and the various terminals throughout the subscriber building. The wire junction box is usually connected by modular plug to the network interface.

The wire junction box allows multiple connections of telephone station wire throughout the building. The AT&T standard wire junction box is the model 742B, which allows the user to connect up to three sets of station wire to modular jacks throughout the residence or small business.

The wire junction box is the first access point that the operative can rely on to be free from detailed inspection by TELCO service technicians. If you are able to access this box (it is usually rectangular and grey or light beige in color, with a regular screw in the center of the outside cover), remove the cover and see if there is a spare terminal from which you can run your parasitic interconnect.

By gaining access to the junction box, the operative will be able to determine how technically compatible the target line is to a number of parasitic devices. All telephone devices consume a specific amount of current from the line. If you hook up a device that consumes too much current, the subscriber's phone may be affected. It may not ring as loud or it may have a recognizable drop in the audio level he hears. This potential problem is not common, but it could be if you intend to hook up a device for eavesdropping such as a radio-controlled tap that uses the phone line voltage to function.

All telephone devices—including fax machines, com-



Internal and external view of an AT&T 742B wire junction box. This device can be purchased from a variety of sources. Note: Junction color code connections may not be in this sequence. Check internal layout and verify color codes on each unit. Also note that if three connections of high-drain equipment are already on-line at this junction box, a parasitic hookup may affect the REN number.

puter modems, answering machines, etc.—are assigned a *ringer equivalence number* (REN), which is marked on the unit along with its FCC registration number. The tag on a typical AT&T phone would read something like this:

Complies with Part 68, FCC Rules
FCC Reg. No. AS52UD-10461-TE-E
RINGER EQUIVALENCE 0.4A & 0.7B
AT&T Technologies, INC.

The two ringer equivalence numbers describe the relative load the phone puts on a line when on and off the hook. Most phone company installations can handle up to 5.0 REN on any given line. (Thus the subscriber could hook up seven of the above phones with no problem.)

If there are three lines of station wire going through the junction box, it may be risky to place certain devices on the line since each station wire may, in fact, go to two or three phones. Most of the parasitic phone taps on the commercial market place a substantial drain on the phone line. These devices are, of course, not FCC registered, and no REN number is provided. Placing such a device on a heavily used line will prevent all the phones in the residence from ringing.

The junction box is a very good location in which to place a device, but the load placed on the line has to be considered. Though overloading a line is rare, it is becoming more of a concern as new devices such as fax machines and computer terminals are hooked up to phone lines. The FCC generally only allows registration of devices that have an REN of 1.0 or less, meaning about five devices usually can be placed on a line with no problem.

In a large apartment building or business location, the wire junction box is much larger, being a board with hundreds of pairs of connections. In most cases, it is surprisingly accessible in these buildings. It is frequently found in a cleaning supply closet in an office building, or in a storage closet or laundry area on the first floor or basement of an apartment.

For surveillance hookups, cable rerouting, and spare-pair interconnection applications, the wire junc-

tion box in these buildings is ideal. The large number of multicolored wires running in and out of these boxes will allow the operative to creatively employ a number of techniques without alerting an untrained observer. A phone company technician may not even notice your work if it is done carefully and employs standard TELCO station wire.

Access to the junction box requires access to the premises. If the target is a residence, the operative will probably be involved in breaking and entering to get to it. If the target is a business or large apartment, the wire junction frequently is in a neutral area, and the only direct risk is trespassing.

Station Wire

From the wire junction box, the phone circuit continues to each phone or modular plug through a four-conductor cable known as *station wire*. This wire is usually grey or beige in color, and can be traced from the network interface or the wire junction box to the modular plug or phone. The wire is 22-26 gauge, unstranded, copper coated, and has a "stiff" feel when handled in the dark. It is often fastened along baseboards with U-shaped staples or nails.

There are some general characteristics of telephone station wire that make it suitable for a variety of parasitic hookups. These include:

1. OUTSIDE INSULATION. This is the jacket on station wire. It is generally grey rubber or plastic, 3/8- to 1/4-inch wide. Braided metal shielding is usually not used as outside insulation. The rubber material is easy to pierce or cut, so inductive probe devices are compatible with this configuration.

2. INNER CONNECTION WIRES. Usually four to six color-coded wires are found inside station wire. These wires are paired for each phone. The most common configuration in 95 percent of American homes is four-con-

ductor *D station wire* in a grey rubber jacket. D station wire has no wire braid between the jacket and the four conducting wires, and the color codes are as follows:

- RED—RING. Connects to the negative side of CO battery.
- GREEN—TIP. Connects to the positive side of CO battery.
- YELLOW—Not used normally, but may be used for second line RING.
- BLACK—Not used normally, but may be used for second line TIP.

D station wire is easy to identify and generally easy to access. In many locations it runs directly out of pay phones, and a pay phone terminal is probably the ideal penetration point. It is used as a drop wire from the phone to the terminal box in this configuration.

Six-conductor station wire can be encountered in some homes. Besides the telephone circuit, it is also used to connect alarm systems and intercoms. Its color code sequence is as follows:

- BLUE with white bands—Corresponds to D style RED.
- WHITE with blue bands—Corresponds to D style GREEN.
- ORANGE with white bands—Corresponds to D style YELLOW.
- WHITE with orange bands—Corresponds to D style BLACK.
- GREEN with white bands—Corresponds to D style RED.
- WHITE with green bands—Corresponds to D style GREEN.

Note that six-conductor station wire has some stan-

dardized characteristics. A solid color with white bands is always the *ring* or negative (-) connection. White wire with colored bands is always the *tip* or positive (+) connection.

One useful characteristic of all station wire is that it is usually installed away from electrical wiring and other noise-generating devices. This makes hookup of microphones to the "spare pair" (yellow and black wires) both an opportunity and a threat to the operative—the relatively noise-free line is easy to monitor, yet a listening device would be easy to detect. As with the junction box, access to the station wire is usually safe from observation from the phone company; however, the operative must gain access to the premises to install a parasitic device on the line.

Accessing the station wire along its route rather than at a junction terminal or plug is recommended. This requires a few tools and a small amount of practice. The fastest and most reliable techniques are insulation displacement and flame splicing.

Insulation displacement applies to several techniques. In this context, it is the method of connecting to a station wire by piercing the color-coded insulation of the internal wires with a large needle and "sewing" in a fine-gauge interconnect splice. It is fast and easy to remove. The tools required for this include:

1. A SMALL, SHARP KNIFE. X-ACTO knives are excellent, but any small pen knife is adequate as long as it is razor sharp.

2. SEWING NEEDLE. The type used for sewing leather goods is fine. Larger cloth needles work, too.

3. WIRE WRAP WIRE. This is thin 30-gauge hookup wire used by hobbyists. If it is not available, laminated 28- to 30-gauge bell wire may be used (though it is necessary to burn off the painted lamination and sand about an inch on each end for good conductivity). Wire wrap wire comes in a variety of colors and quantities from outlets such as Radio Shack.

4. GREY TAPE. This is optional. Standard duct tape is almost exactly the same color as D station wire and can be used to cover the incision if the cut cannot be made on the underside of the wire. Glue can also be used.

The procedure for insulation displacement is as follows:

1. Find an accessible spot in the line and carefully pull on the station wire to raise it about 2 to 3 inches away from the baseboard or wall.

2. Make a light incision with the knife about 1 inch in length along the *underside* of the wire.

3. Use the blunt end of the needle to pull out the red and green wires about 1/4 inch from the inside of the jacket. It need not be out too far for the job.

4. Thread the needle with the wire wrap wire or laminated bell wire. Push the tip into the insulated red wire and feel the solid metal interior. Pull the stripped wire wrap wire back through and remove it from the needle. Tie it securely in place. Do the same for the green wire. WARNING: If the phone rings during this step, you will receive a painful but nonlethal shock. It may, however, cause you to yell out, revealing your presence.

5. Carefully place the wire wrap wire behind the station wire and feed it along the same route to the parasitic hookup and verify function. HINT: Marking each wire wrap wire red and green or using color-coded wire eliminates the need to verify polarity.

6. Push the red and green wires back in the jacket, remold the wiring in the jacket, and close the incision with a dose of super glue. Before the glue dries, push the cut side of the station wire against the baseboard or wall. The glue will cause your parasitic hookup to be completely concealed and difficult to locate.

Once function is verified, this parasitic hookup can be used from anywhere close-by. If the station wire is in carpet, the wire wrap wire can be sewn right through the lower pile of the carpet. This approach is useful if, for example, the parasitic hookup is run from the spare pairs

(black and yellow wires) to a microphone under a table in the target room.

Insulation displacement takes a great deal of practice. Purchase some station wire from an electronics store and do some mock installations before attempting it at an active location. Practice this technique crouched down on your knees, since in most cases you will be doing so in a real scenario. Have your wire prepped and ready and check your tools. Verify that the glue will flow easily. Make sure the knife is scalpel sharp. The needle can be sharpened on an emery board—the sharper the needle, the easier the insulation displacement is to execute.

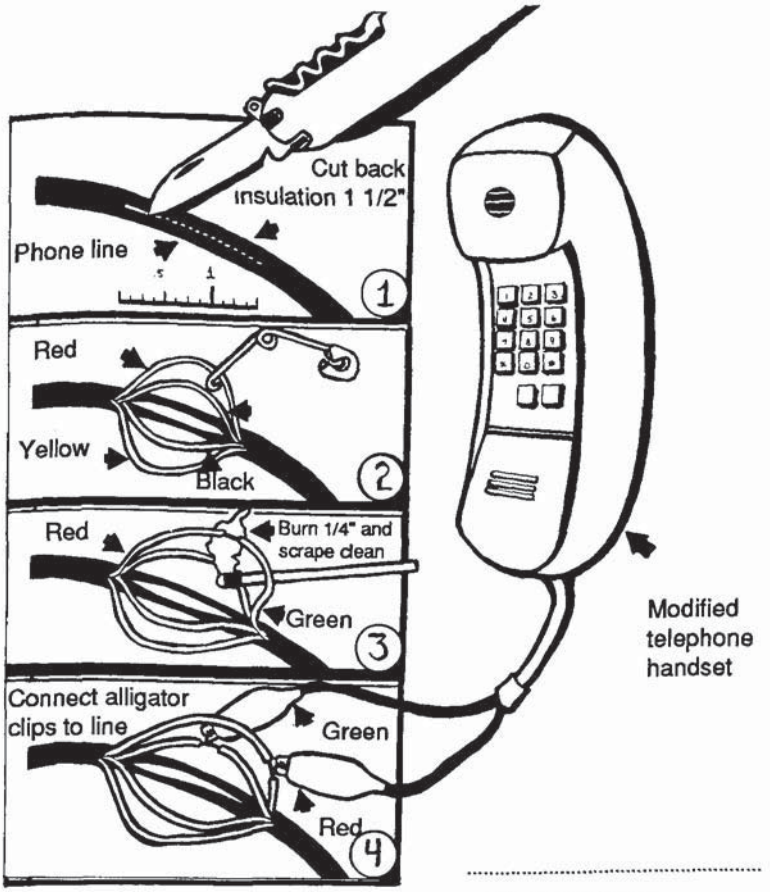
Insulation displacement of station wire has many applications, from pay phone parasitic hookups to telephone taps and audio surveillance work. It is difficult to detect and, when done properly, is fast and reliable.

Flame splicing is for outdoor applications. The operative gains access to the station wire feed from a pay telephone or interior run and performs this maneuver to gain access to the line.

Tools required for flame splicing include:

1. X-ACTO KNIFE.
2. LIGHTER OR MATCHES. Matches are easier to use.
3. MODIFIED SAFETY PIN. Use needle-nose pliers to bend a hook on the tip of a large safety pin, as shown in the illustration on page 179.
4. ALLIGATOR CLIPS. These should be connected to the modified handset telephone.

Flame splicing generally is a fast temporary hookup—the operative can teach it to specific cell members to defeat a pay phone, for instance. Flame splicing should not be employed indoors, where it will produce a characteristic odor that is hard to remove. The technique is risky to perform at night, and it also temporarily denies the operative his night vision.



Flame splicing.

Flame splicing is executed as follows:

1. Locate and access the station wire. Make a 1- to 2-inch incision in the grey jacket with the knife.

2. Use the modified safety pin to pull out the green and red wires about 2 inches from the jacket.

3. Use a match to burn off the rubber insulation on the red and green wires about 1/4 inch. Do this at two different points along the wires: if the splice on each connection is too close together, the wiring will short out and

cause the connection to fail, which will call the attention of service personnel. NOTE: The station wire will burn *very fast.* Blow out the flame as soon as it "catches" on the insulation. It will burn a quarter inch in less than a second from ignition.

4. Using the back of the knife blade, scrape the burned plastic and soot from the wire. Connect the alligator clips and make the call.

5. When you are finished, push the wires back in the jacket and remold the jacket to conceal access.

Flame splicing can also be performed on drop wire and other connecting cables, and it is good for quick access to alarm wire and sensor feeds. The technique requires practice and knowledge of the burning characteristics of the insulation around the wire.

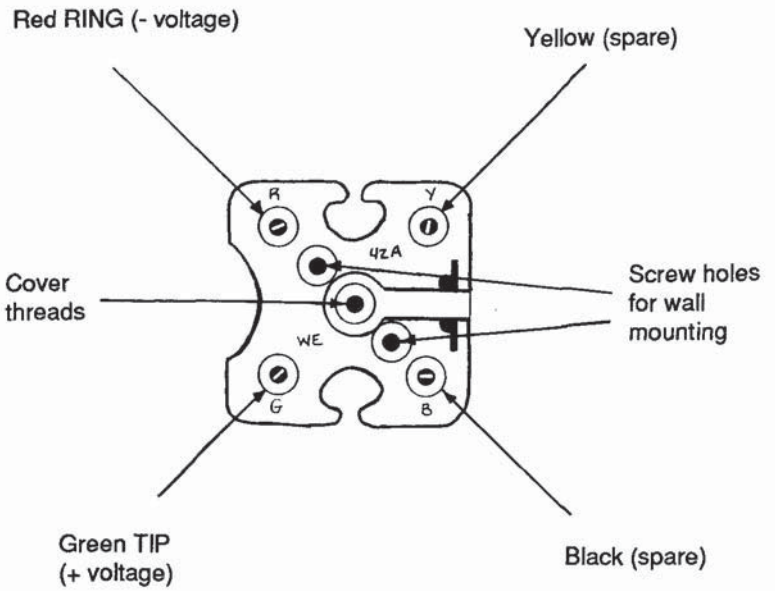
Modular Plug

The station wire runs from the junction box to a plug-in jack known as a *modular plug.* Since 1974, the telephone company has used these types of plugs to install telephone systems.

The standard AT&T modular plug is the model 725A. This surface-mounted modular jack can be found in most American homes. It is common to insert a small microphone inside the jack's housing and put a small hole in the underside of its faceplate so air can circulate freely and provide audio to the mike.

Access to a modular plug is seldom possible without risking OPSEC. However, there are characteristics of the modular plug that make it a useful access point for parasitic interconnects.

1. PROXIMITY TO TARGET. An audio microphone running the route of the black and yellow spare pair can be installed inside every modular plug in a residence. This is an excellent means of collecting voice data. Routing the microphones to a nearby junction box and then to a radio or infrared device allows the operative to



Modular plug commonly found on most homes in North America. Illegal extensions and line bugs are connected to red and green points. The "spare pair" yellow and black connections can also be used to "wire" a building or residence with listening devices.

bypass a countermeasures threat because the actual transmitting device is not in the room, only the microphone is. The spare pair wires can function as a long wire antenna for the listening device to give it extended range.

2. PROTECTION. When a telephone transmitter is installed directly inside the modular phone jack, it is indoors and thus protected from the weather. It also is concealed from view inside the jack (and telephone company personnel do not generally get near this jack during their service work). This eliminates several operational threats.

The disadvantages of working with the modular plug should be obvious. If you have gained access to the mod-

ular plug, you have probably gained access to the premises illegally. Besides, if you have access to the modular plug, you also must have access to the actual telephone and can simply make your call from it. Therefore, the station wire is the last realistic access point available to the operative. The modular plug is more suited for surveillance/collection ops.

Both the wire running to the phone and the phone itself can be used in surveillance applications, but they are extremely vulnerable to physical inspection. Service theft at this point is not recommended.

Hardware for Telephone Circuit Work

The essential tools for telephone service theft will vary from operation to operation. The tools and equipment described in this section are intended to fulfill a variety of access and surveillance needs.

As stated earlier, parasitic interconnect is quite similar to telephone tapping in both access points and procedure. The wiretapping specialist is known in the intelligence community under a variety of titles and descriptions, from *electronic surveillance operative* (ESO) to *wireman*. These terms describe an experienced electronics technician who specializes in phone communications intercept and countermeasures.

Before discussing the tools, hardware, and techniques of this specialized occupation, something has to be clarified to the operative. Possession of the tool kit described in the following pages is illegal in any jurisdiction if it can be established that it is to be used for intercepting communications by wire or for attaching foreign devices on a commercial telephone circuit. Operatives have been caught and convicted of simple possession of this type of hardware and imprisoned for many years. In fact, there are cases that involved no physical possession of this hardware but simply the "intent" to possess and use it. A quick review of U.S.

case law regarding this equipment may help you in your OPSEC planning.

In 1969, a legendary wireman was arrested and convicted of "conspiring to provide technical information about electronic eavesdropping techniques." Bernard R. Spindel was one of the best telephone surveillance specialists in the world. He was trained by the U.S. Army Signal Corps and served in the Office of Strategic Services (OSS) as a specialist in wiretapping during World War II.

Spindel perfected the art of electronic telephone intercept by bringing the hardware into the transistor age. He worked in and out of government and private circles for years after the war. He served as technical advisor to the New York City Anticrime Commission with William Donovan (former director of the OSS and one of the founding fathers of CIA). Spindel's career has been unequaled in the wiretapping field. His creative expertise in the craft brought government, business, and even organized crime to his doorstep for advice and assignments throughout his life.

Most of Spindel's government and private assignments were for illegal wiretaps. In fact, according to the U.S. government, Spindel was so good at what he did that even when it had solid testimony on his activities, none of his wiretaps could be traced back to him. What finally put Spindel in prison and ultimately ended his career is something that all operatives should consider very carefully.

In 1969, a licensed private investigator was retained by a wealthy heir to the A&P grocery store chain by the name of Huntington Hartford. Hartford suspected that his wife was having an affair, so he retained the investigator to bug his wife's apartment and tap her phone. The investigator was not an expert on the subject of wiretapping, but he had done it several times with fairly good results. Nonetheless, he asked Bernard Spindel for some technical advice.

Spindel did not install the tap, build any device for the investigator, or monitor any recordings that the investigator made. Spindel only gave advice as a favor. Upon doing so he committed a felony, as it was (and is) a crime to even discuss the technical aspects of a wiretap with another individual. Spindel was convicted and sent to prison.

It is a crime to possess or sell any device that is intended to be used for eavesdropping or wiretapping. If you are caught transporting any such device, tools, or hardware across state lines, you have committed another felony. There is little legal difference in U.S. case law regarding the intentional placement of any "foreign device on the commercial telephone system" for collecting information or stealing service. In other words, if you are caught in the act of possessing tools that enable you to use the commercial phone lines illegally, you may also find yourself charged with illegal wiretapping. If you are caught even *discussing* such activities, as in the case of Bernard Spindel, you can be arrested, charged, and convicted of violating Section 801 of Title III of the U.S. Code w(1)g, which relates to "conspiracy to provide technical information about electronic eavesdropping techniques."

Thus the most significant risk involved with parasitic interconnect is that it involves the commission of a number of serious crimes. This risk should not be underestimated. A parasitic interconnect will be prosecuted under its own statutes, but the *method* you employ is in fact prosecutable under the above federal title. You will not have the legal defense of claiming you were only making a free phone call. You will probably be charged with both crimes. Discussing your techniques, "showing off" your tools or equipment, and teaching others how to employ these skills are all federally prosecuted criminal acts.

The point is that failure to carefully consider the legal ramifications of the employment of these techniques, possession of these tools and devices, and the casual

"sharing" of this information will result in your entire operation being burned. Individuals caught and convicted of conspiracy in this area have been sentenced to longer prison terms than individuals caught carrying concealed automatic weapons, building and using homemade silencers, and illegally transporting explosives. As you collect your tools and develop your skills, keep in mind that you are already committing a crime even before you attempt your first parasitic hookup.

Possession of this manual along with the tools described herein will be probable cause for a search of your premises and surveillance against you. Depending on your situation, the act of reading this manual alone could be considered the act of conspiring to violate a criminal statute. This is not meant to intimidate as much as it is to inform you. Collecting the hardware is what puts you on the other side of the law. Proceed with caution.

• • • • •

The tools required to conduct telephone service theft and wiretapping must perform the following three tasks:

1. CONSTRUCTION OR MODIFICATION OF SPECIALIZED EQUIPMENT TO HOOK UP ON THE PHONE CIRCUIT. Electronic kit building, disassembling and altering telephone equipment, fabricating connecting jacks, and so forth must be accomplished.

2. CIRCUIT ACCESS. This includes splicing, testing, and analyzing lines, gaining entry to enclosures and premises, and installing the parasitic device.

3. STERILIZATION. This includes "cleaning up" installations, avoiding signature impressions, taking counterdetection measures, and so on.

Combining these three prerequisites with the need for the tool kit to be concealable and functional requires the careful consideration of each item in the kit. Fortunately, there are a number of "combination" type tools available

that can help in this regard. In fact, the entire kit can be carried in pants pockets if the following items are selected.

1. VICTORINOX "SWISSCHAMP" SWISS ARMY KNIFE.
2. LEATHERMAN "MINI TOOL" UTILITY KIT.
3. PORTASOL BUTANE SOLDERING IRON.
4. THIN SOLDER.
5. ELECTRICAL TAPE.
6. SAFETY PINS.
7. RUG-SEWING NEEDLE.
8. PENCIL WITH ERASER.
9. PAPER CLIPS.
10. BECKMAN POCKET-SIZE VOM MODEL "CIRCUITMATE DM78" WITH PROBE KIT.
11. AT&T TELEPHONE LINE TESTER AND INSTALLATION TOOL, MODEL 953B.
12. PELICAN "MITY LITE" PENLIGHT WITH RED LENS FILTER.
13. TWO-FOOT SECTIONS OF 24-GAUGE RED, GREEN, BLACK, AND YELLOW WIRE.
14. ONE 20-FOOT ROLL OF 30-GAUGE WHITE WIRE WRAP WIRE.
15. DISHWASHING GLOVES.
16. FIFTY FEET OF FOUR-CONDUCTOR STATION WIRE, AT&T STANDARD D (OPTIONAL).
17. INSULATED ALLIGATOR CLIPS, SMALL AND MEDIUM SIZE.
18. SUPER GLUE.
19. RUBBING ALCOHOL IN NASAL INHALER BOTTLE.
20. Q-TIPS.
21. MODULAR PLUGS (OPTIONAL).
22. SPLICING TOOLS (OPTIONAL).

OPSEC is a major consideration in selecting the above tools. Most of them are not suspicious to own or use, have "innocent" applications, and are less incriminating than some of the alternatives.

Victorinox SwissChamp Swiss Army Knife

This is the largest Swiss Army Knife made. It has a total of twenty-nine tools, many of which serve more than one function. The entire unit weighs about 6 ounces and can be placed in a Cordura nylon case that fits on a belt or in a pocket nicely. It is insulated with a plastic covering for safety.

Here is an inventory of the tools contained in this tiny package:

1. LARGE KNIFE BLADE.
2. SMALL KNIFE BLADE. Useful for station wire incisions.
3. CORKSCREW.
4. CAN OPENER.
5. BOTTLE OPENER.
6. SMALL SCREWDRIVER. Perfect size to open modular plug boxes and junction boxes.
7. LARGE SCREWDRIVER. For opening terminal boxes and network interfaces.
8. PHILLIPS HEAD SCREWDRIVER. Good size for opening handsets, etc.
9. WIRE STRIPPER. Works well on station wire.
10. REAMER. Its sharp point can be used to put a small hole in the modular jack for microphone installation.
11. SCISSORS. Can be used to cut and strip wire.
12. MAGNIFYING GLASS. Excellent for verification of solder joints.
13. WOOD SAW. Can be used to cut access holes in dry wall or wood.
14. FISH SCALER.
15. NAIL FILE.
16. METAL FILE. Useful for sanding lugs and connections for soldering.
17. METAL SAW. As good as a hacksaw for removing padlocks or cutting chain link fence for access.
18. FINE SCREWDRIVER. About 1/8-inch wide.

Victorinox SwissChamp. (Illustration courtesy of Mark Camden)

Good for terminal box wiring and screws inside jacks.

19. MINI SCREWDRIVER. This tiny 1/16-inch-wide insulated tool is in the corkscrew and can be used to fine-tune listening devices, etc.
20. KEY RING. Attach your four sets of two-foot wire sections to this.
21. TWEEZERS. Useful for "heat sink" applications when soldering.
22. TOOTHPICK. This can be jammed down in a hook switch to keep the phone on the hook while "servicing" the handset.
23. CHISEL.
24. PLIERS. These can be used to remove 1/4-inch nuts and for soldering.
25. WIRE CUTTERS.
26. BALLPOINT PEN. For making quick notes about wiring layouts before doing any creative rerouting at a junction box.

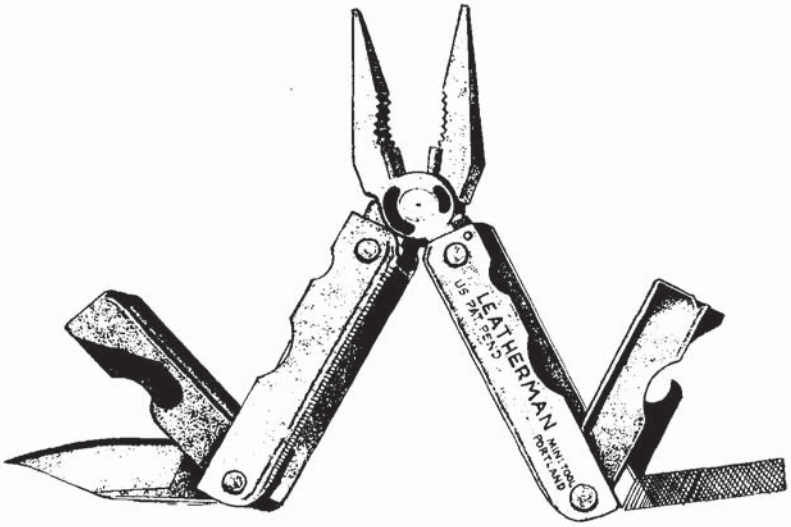
As you can see, this small tool can be used in a variety of tasks. Of course, like most combination tools that have many functions, this one is not perfectly suited to any one task—it does a lot of things fairly well. Practical limitations experienced with this tool include the wire cutting and gripping ability. For this you need another combination tool.

Leatherman "Mini-Tool"

The Leatherman Mini-Tool is an extremely durable fold-up tool that comes with a twenty-five year warranty. It has more heavy-duty applications than the Swiss-Champ, which makes it a good addition to a kit. Here are the tools on the Leatherman:

1. SMALL KNIFE BLADE.
2. HEAVY NEEDLE-NOSE PLIERS. These can be used to hold circuit parts as well as remove up to 3/4-inch lug bolts.

3. WIRE CUTTERS. These will cut *any* type of electrical wire. They will also cut barbed wire and chain link fence.
4. FLAT-TIP SCREWDRIVER. If a screw is set tightly, this driver is strong enough to loosen it, where the SwissChamp may not be able to handle the strain.
5. FILE. This heavy-duty file can be used on most hard metals.
6. CAN OPENER.
7. BOTTLE OPENER.

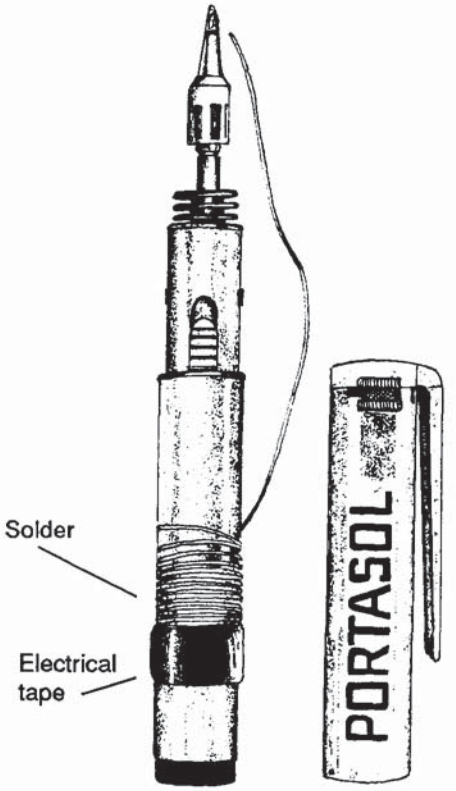


Leatherman Mini-Tool. Excellent for illegal phone work. (Illustration courtesy of Mark Camden)

The Leatherman Mini-Tool folds up into a 2 1/2 x 1-inch package that fits into a small Cordura nylon pouch, which has an extra internal pocket for a small amount of wire, solder, or folded 3 x 5 cards for note taking. It does not perform nearly as many of tasks as the SwissChamp, but it does bet-

ter at those tasks that it is designed to do. A rubber band around the grip allows the operative to use the Leatherman's pliers as a minivise to hold tiny circuit boards or parts while soldering. Wrapping a layer of electrical tape around the grip creates an insulated pair of pliers for working safely with the heavy lugs on a terminal box.

With the Leatherman and the SwissChamp, you have over thirty-five different tools available in your pocket.



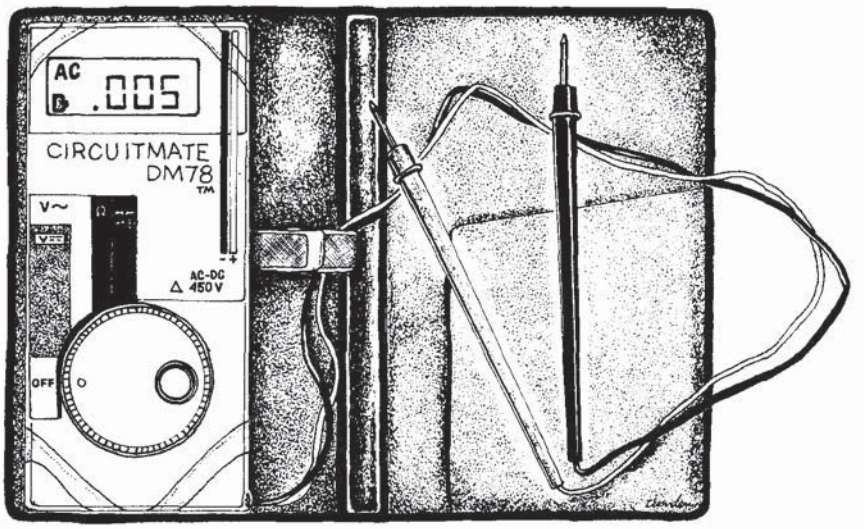
The butane-operated Portasol is an excellent field tool for soldering wire taps and parasitic devices covertly anywhere along a phone line. (Illustration courtesy of Mark Camden)

Portasol Butane Soldering Iron

This is a small, portable soldering iron imported from Ireland. It has a variety of tips, including large and small soldering tips, a cutting tool, and even an attachment for welding. A "clone" model of this tool is available from Radio Shack.

The Portasol is 7 inches long and 3/4-inch wide, about the size of a large Magic Marker. It is self-contained with a flint striker on the cap. The fuel regulator and refill nozzle are on the bottom of the main unit. The Portasol comes with a clip on the lid that allows it to fit in a shirt pocket and is light enough to be carried on every job.

In telephone work, you may want to solder the parasitic device directly on the line. For this you can wrap a small amount of solder around the main body of the Portasol. The finest-gauge solder available is recommended (such as Chemology 60/40 .031 inch). Several feet of electrical tape can be wrapped around the handle of the iron for quick use, since after soldering you will want to tape the connection.



The tiny Circuitmate DM78 is an excellent pocketsize VOM for checking continuity, verifying line voltage, checking if a line is in use, etc. Precise measurements can be made quickly even while working on a telephone pole. (Illustration courtesy of Mark Camden)

The optional knife blade for the Portasol can be used to cut through any type of plastic quickly. This is particularly useful in Europe and some newer phone company installations where the network interface is locked or secured. This "hot knife" is also useful for equipment modifications and accessing TELCO terminals.

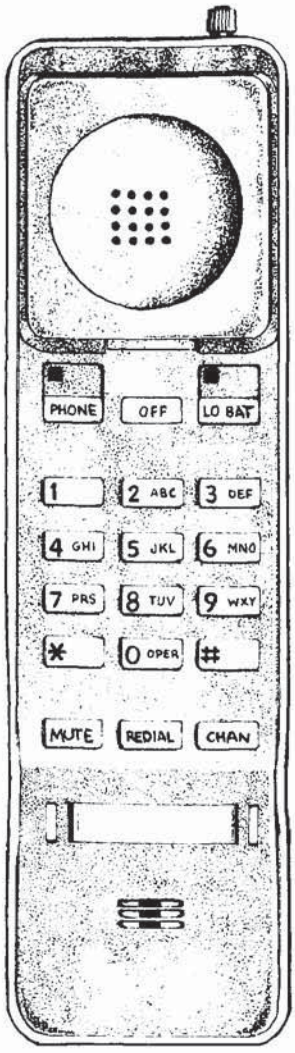
The Portasol can be adjusted to solder with a small amount of heat or with a very high temperature for lug connections. I have been soldering various components for more than twenty years using different soldering irons, but the Portasol has been the only one in my kit for three years now. It is extremely reliable, heats up to melting temperature in about thirty seconds, and works well outdoors as long as you shield it from high winds when igniting the fuel regulator cell. The Portasol is refillable with any type of cigarette lighter butane can, and it will run for over an hour on one filling. A damp rag is handy to wipe off the tip as you solder so it will heat up quickly at every ignition and last a long time. This unit is a low-maintenance, compact tool good for a variety of jobs.

Beckman VOM Model "Circuitmate DM78"

This is an inexpensive multimeter that is smaller than many fold-up electronic calculators. It is used to determine if a line is functional, is currently in use, or if a parasitic device is properly installed. The high-impedance sensory characteristics of this VOM (volt ohm meter) allow it to be connected to an occupied line with no telltale "clicks" heard by the user on the line.

The Beckman requires a small lithium "button cell" battery that lasts many months. The unit has a low-battery indicator and an audible continuity-indication piezobuzzer. The digital meter is more fragile and actually slower in response than an analog multimeter, but it is more accurate and seems to hold up better in high humidity since there is no mechanical movement to consider. The meter is also much lighter and less bulky than an analog unit. Still, many operatives prefer an analog meter for pole climbing (such as a cheap Radio Shack pocket model) because it is faster and, if dropped, costs less than $10 to replace.

Pocket-size VOMs are available at Radio Shack stores



The AT&T HT-5200 cordless phone handset can be used as part of a covert line seizure when the base unit is modified as outlined in the text. (Illustration courtesy of Mark Camden)

and from many mail-order outlets. The choice of digital or analog type is up to the operator.

AT&T Line Tester and Installation Tool, Model 953B

This small, inexpensive tool is the Swiss Army Knife of telephone line installers. Designed by AT&T for use by home installation do-it-yourselfers, it is pocket size and easy to use. It can test a line and hookup for function and verify that an installation is properly performed. It verifies line polarity, and the back of the unit has a wire-stripping tool. The tester plugs directly into a modular jack. A VOM can perform the basic functions of this device, but the 953B is faster for "go/no go" tests. A simple modular plug modification allows this handy tool to be used outdoors at night.

Pelican "Mity Lite" AAA Penlight

This extremely durable penlight is bright and powerful. It uses a xenon bulb instead of a normal incandescent bulb (xenon is used in flashbulbs on cameras). The Pelican Mity Lite was designed to FBI specifications and has a small magnetic end so

it can be placed on a metal surface while the operator works. It is durable, waterproof, and can be turned on and off with one hand.

Field Techniques for Line Seizure

There is a suitable telephone line to seize on virtually every street corner and in every building in North America and Europe as well as most parts of the rest of the world. A city contains literally millions of access points at which line seizure can be effected.

The following are the sequence of events of line seizure:

1. PREMISSION SURVEILLANCE. During the day, select a site along a seldom-traveled path. Make careful note of traffic, vehicles parked in the area, street lighting, and residential windows from which observation could occur.

Note escape routes that permit only foot pursuit, thus limiting vehicular pursuit. Most ops of this nature will be conducted at night, and the target line will belong to a business subscriber. This limits risk and permits access to an area that is quiet after business hours.

2. EQUIPMENT PREPARATION. Note the type of access point and its physical characteristics. Do a "walk through" on a mock-up so you know exactly what you wish to accomplish. Have all equipment concealed yet instantly accessible. With the right gear and skilled hands, line seizure should take no longer than two minutes unless a pole must be climbed. Cordless phone or radio tap devices can be wired and emplaced quickly if the actual conditions for installation are considered carefully.

3. TEMPORARY COMMAND POST. This is an area that will allow visual observation of the target site prior to seizure and during actual use of the line. The CP can be a vehicle parked some distance from the target access point.

Surveil the area and have the equipment ready to go. Hook up and go back to the CP to make calls. Line of sight allows good radio signals to be sent back to the CP while

providing a degree of physical surveillance of the area and target terminal.

4. PREPLANNED CONTACTS AND CODES. Once "on-line," make the calls brief and concise. *Assume you are being monitored.* Use all protocols and codes clearly and get your message through as quickly as possible. If you are conducting a pay phone call, use another pay phone to arrange the call with your contact, then go to line seizure to call the specific pay phone. Do not discuss methodology or line seizure over the telephone, ever.

5. EXTRACTION. Once contact is complete, observe the target area for a possible ambush. Go to the hookup, restore the subscriber line, retrieve all equipment, and police the area visually for any tools or marks left at the scene. Never use the same target line twice. Maintain a substantial distance between each seized access point. Do not develop any identifiable pattern in line seizure such as always hitting a specific type of terminal box or network interface.

Modified Cordless Telephone Set

A cordless telephone is a two-way radio link between a base unit and a hand-held telephone. The base unit is connected to the telephone line, generally through a modular jack in the users residence. Ten million cordless phones were sold in the United States in 1989.

Making four simple field modifications to a cordless phone will allow it to be hooked up outdoors next to an accessible terminal box on a pole or a network interface. It can be quickly mounted, wired, and operational within minutes. It can be modified to extend its effective range to several city blocks, and the entire unit can be left unattended until another contact is required.

The four modifications required are:

1. Connection to a DC power source.
2. Redesign of base unit antenna for extended range.
3. Modification of input jack for direct wire hookup.

4. Encapsulation of base unit housing for outdoor use.

In order for the finished product to be useful and fully functional, it is important to start with a good basic unit. The market has been deluged with many models of cordless telephones, but those manufactured after 1988 tend to be of higher quality and are more reliable than earlier models.

One make of cordless telephone that is well made and seems to be extremely durable is the AT&T HT 5200. It is an excellent cordless telephone for parasitic application. The base unit's power supply is a wall transformer that is already external to the base. This unique design feature makes field modification quick and easy. The external power supply is a twelve-volt DC 200mA unit that connects directly to the base unit's main printed circuit board through a rubber grommet next to the modular jacks and base antenna at the top of the unit.

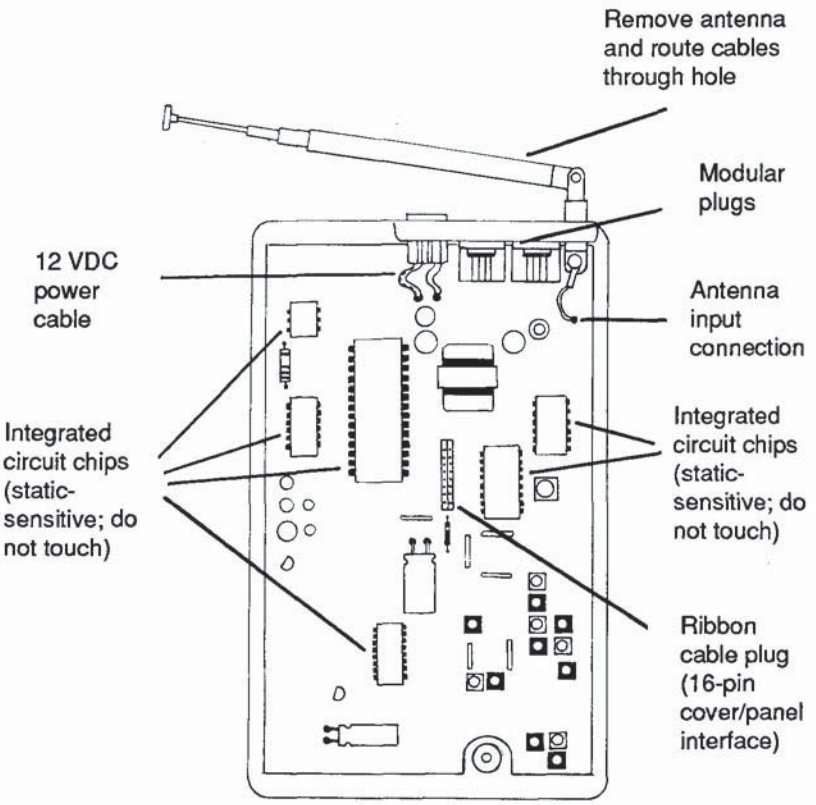
The modifications to make the HT 5200 suitable for outdoor line seizure can be done in about fifteen minutes with the following materials:

1. RADIO SHACK MODEL 270-407 EIGHT AA BATTERY HOLDER.
2. TWENTY FEET OF D STATION WIRE WITH MODULAR PLUG ON ONE END.
3. TWO MEDIUM-SIZE ALLIGATOR CLIPS.
4. ONE ARMY SURPLUS 7.62MM M13 200-CARTRIDGE AMMO CAN (10 x 7 x 4 inches).
5. HOOKUP WIRE.
6. SOLDER.
7. TAPE.
8. PORTASOL SOLDERING IRON.
9. SMALL PHILLIPS HEAD SCREWDRIVER (Victorinox SwissChamp works fine).

Modification is fairly straightforward. Start by preparing the station wire. The grey-jacketed AT&T D station wire will function as both an interconnect and a long-range antenna for the HT 5200. Connect a modular plug to the red and green wires on one end of the 20-foot sec-

tion of station wire. On the other end, hook up two insulated alligator clips. These two clips do not have to be red and green in color, but they should be connected to the red and green wires, and the corresponding color codes should be noted. Also, strip one end of the yellow station wire to function as an external antenna.

The Radio Shack AA battery box has a standard clip connection for a nine-volt DC transistor radio battery. Bypass this connection on the underside of the unit


Remove antenna and route cables through hole
Modular plugs
12 VDC power cable
Antenna input connection
Integrated circuit chips (static-sensitive; do not touch)
Integrated circuit chips (static-sensitive; do not touch)
Ribbon cable plug (16-pin cover/panel interface)

View of circuit board of AT&T HT-5200 cordless phone base unit.

and connect two pieces of hookup wire to the terminals. Install the batteries and test the connections for 12 volts DC.

Open up the bottom of the HT 5200 base unit by removing the four Phillips head screws on the underside of the case. Gently lift off the cover and pull it to the right. There is a sixteen-pin ribbon cable that connects the faceplate to the main printed circuit (PC) board. Carefully unplug this unit.

This PC board is well constructed and durable, but there are some important handling rules that must be considered. On the PC board are six integrated circuit chips as well as a number of transistors and other semiconductors. *Do not touch these chips.* The small amount of static electricity in your body could easily damage these sensitive units. The basic rule of thumb for working around PC boards is to have clean, dry hands and good lighting.

Note at the top right that the antenna, power jack, and modular phone jacks feed into the PC board from the outside of the case. Use your Phillips head screwdriver to remove the antenna from the PC board; connect the yellow lead from the station wire to this terminal. Ensure that the antenna connection to the PC board is still intact. Plug the modular jack into the modular plug and the station wire is installed.

Solder the battery leads to the terminals where the external power supply feeds into the PC board. Make sure the polarity is correct. (You may feed the station wire and the battery connections into the hole left by the removed antenna.)

Verify all connections for good solder joints and plug the sixteen-pin ribbon cable back into the main PC board. Put the unit back together and replace all four screws in the bottom.

Connect the alligator clips on the other end of the station wire to a working line and attempt to make a call with the remote unit. If everything has been connected properly, you should be able to use the phone. Note that

you do not cut the normal power supply wires from the PC board. You want to keep the plug-in supply with the unit so you can recharge your remote battery cells from a plug. (When recharging the remote or when using the modified unit with AC, make sure you remove the batteries from the battery box or they will be damaged and possibly explode from the 12 volts DC from the adapter.)

The HT 5200 with remote, station wire, and battery box will fit snugly inside a standard 7.62mm military ammo can. This provides the unit with a tough external case for transport and weather protection for outdoor deployment. (NOTE: These ammo cans cost a couple dollars on the surplus market, but it is important to make sure that the rubber seal around the lid is intact and in excellent condition. Prior to deployment, place newspaper in the can, close it up, and submerse it in water for at least an hour. If the newspapers remain dry, then the integrity of the seal is still good.)

Field deployment is simple. Find a telephone pole in a remote area at night. Climb up, access the terminal box, bypass the subscriber, hook up the clips, and feed the grey station wire down the pole. You can bury the ammo can at the base of the pole since the antenna is enclosed in the station wire running up the pole. In open terrain, this particular model of cordless phone will work almost a half mile away from the pole when hooked up in this manner.

When accessing a network interface in an urban setting, it is important to run the station wire up the side of the building to allow the antenna to perform well. This phone will function for over three blocks as long as there are not a lot of metal obstructions between the user and the installation.

The modified cordless telephone is the ideal parasitic line seizure device. It can be deployed quickly, and the operative can be some distance from the installation while using the line, providing an extra degree of physical security. Most significantly, this simple device is suit-

able for rural underground ops, where the communications officer can perform the installation at a remote telephone pole and the commander or user of the phone can stay concealed. Rural telephones are seldom overly reliable—if parasitic hookup is done at night and the line is restored afterward, the "system" is unlikely to detect the penetration quickly. In an emergency, the unit can be left behind or grabbed quickly by yanking the station wire from the pole while running with the ammo can.

Wire Junction Box Rerouting

A reliable technique for line seizure in a large building is simply to access the wire junction box. As mentioned, this large panel is usually located in the basement of an apartment building or in a common area of a building; this is so the phone company technician can gain access to service the box without impeding the normal flow of foot traffic or requiring someone with a key to let him in. This makes the wire junction box an ideal access point for the underground operative.

Additionally, the typical wire junction box has what many line technicians call "spaghetti" coming from the board as a result of different linemen from the phone company and independent firms connecting a variety of wiring configurations to meet the needs of the building occupants. The addition of an extra pair of "specification" wiring on the board is difficult to detect.

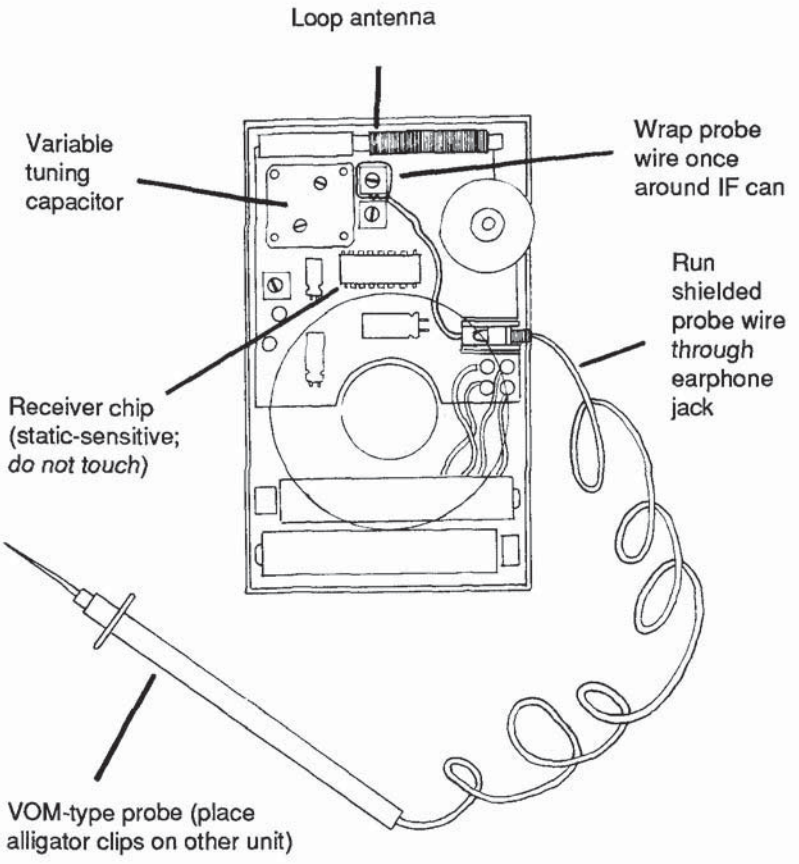
The fundamental problems in the practical application of this technique tend to be locating an unused pair of cables at the junction box and determining where the desired pair actually goes in the building so the operative can employ the parasitic device at this location. Tracing telephone station wire through a building is difficult even for a phone lineman. Less than half of all wire junction boxes have routing plans or markings on them designating which specific station wires go to which rooms or apartments in the building.

The TELCO line technician has a specialized piece of equipment to assist him in this task. The device is basically a small radio frequency (RF) generator that is placed on the line in the room. The technician then places a sensor near the wiring on the junction box that detects the RF field being sent down the station wire from the room. When the sensor is close to the wire connected to the RF device, it gives the technician a tone or light indication, allowing him to locate the specific line in seconds, even on a wire junction board with hundreds of lines. This is a useful technical capability for the operative to have. Unfortunately, these devices are difficult to obtain and extremely expensive.

If the junction box is a simple twenty-five- to fifty-terminal unit in an apartment building, the operative can simply short out the black and yellow station wires at the target room and then trace this wire by checking the resistance of all the black and yellow wires at the junction box until he locates the desired pair. On larger or more elaborate unmarked junction boxes, the following home-built device can be made that will "chase" several thousand feet of station wire through a building or series of buildings. It can be attached to a target line in a room and the operative can locate the specific desired pair of wires at the terminal box in seconds.

The *improvised line discrimination oscillator* described here generates a small amount of amplitude-modulated RF noise that is readily detectable by the sensor unit when placed close to the line. It can be used on active or dead lines with equal efficiency. The unit functions similarly to a wireman's standard line trace unit, only it can be made in about twenty minutes for less than $15. All that is required are two duplicate portable battery-operated AM radios, about 4 feet of hookup wire, an alligator clip, and a VOM-type probe.

The inexpensive AM portable radio in the illustration on page 203 is a Panasonic model R-1007, which costs


Loop antenna
Variable tuning capacitor
Wrap probe wire once around IF can
Run shielded probe wire *through* earphone jack
Receiver chip (static-sensitive; *do not touch*)
VOM-type probe (place alligator clips on other unit)

An improvised line-discrimination oscillator. Using two ordinary, inexpensive AM radios, a low-power RF signal can be sent down a target telephone line by one unit and electronically "chased" and tracked by the other.

about $6 in any discount department store. Any portable radio of this type will work just as well.

Feed a length of hookup wire through the hole in the earphone jack to the *intermediate frequency* (IF) "can," which is a rectangular metal boxlike component on the printed circuit board. Most AM radios have several of

these IF cans on the PC board, and any one can be used for this application. Strip the hookup wire about one inch and wrap it once around the outside of the IF can. Make sure that the connection is tight and well-secured; this can be accomplished by tying the wire together and pushing it down to the bottom of the circuit board.

Perform this simple connection on both radios and close them up. Now tune one radio all the way to the end of the dial (1620 Khz, or 160 on the dial) and tune the other to around 100 (1165 Khz is the exact desired frequency). As you tune the second radio toward 100, you will hear a loud, somewhat irritating whistle from the speaker of both units when the IF frequency of 455 Khz difference is reached between both radios.

When the two probe wires are close to or physically connected to each other, this whistling will be very pronounced. Connect one of these units to a phone line by alligator clipping the probe wire onto the yellow or black wires of the station wire or at the modular plug. Use the other unit to "follow" the signal electronically down the wire.

Note that when the second unit is close to the station wire that has the first unit connected to it, the whistle sound is heard in the speaker. The telephone station wire is now acting as a long wire antenna for the oscillations being generated by the AM radio connected to it.

The yellow or black wires are preferable to the red or green wires because the yellow and black wires generally are not active lines. If the improvised line discriminator is placed on an active line that is currently in use, it will generate an identifiable noise on the line that the subscriber may detect as something suspicious. If this is not a concern in your application, any of the four wires can be used to function as the tracing wire.

This fast, simple, low-cost device works because all modern radio receivers employ a detection circuitry characteristic known as *superheterodyne*. This means that a receiver is also a low-power transmitter—it oscil-

lates at an intermediate frequency as a part of its signal detection process. When two radios of like band are close to each other and their tuned frequency is exactly the IF frequency apart (455 Khz), they tend to whistle, or "heterodyne," against each other. This effect is more pronounced with cheap portable AM radios due to the lack of selectivity and stability of the circuit.

The improvised line-discrimination oscillation unit can be employed in a number of covert communications tasks. It has obvious applications for line seizure, such as allowing the operative to locate a specific pair of wires anywhere on the line circuit, but this capability is also useful in wiretapping.

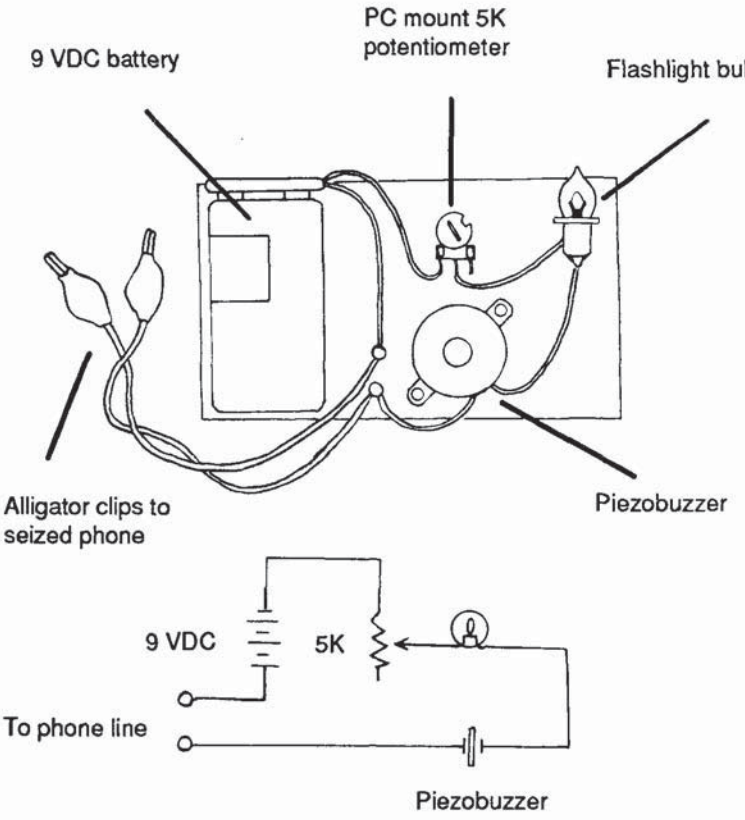
Another useful characteristic of a portable AM radio wired in this configuration is that it can be used to detect a number of devices that might be covertly placed in an area. For instance, modern surveillance video cameras are small enough to fit inside a cigarette pack, and the lens aperture can be as small as 1/8 inch in diameter. Yet any video camera will produce identifiable oscillations. The operative can use an AM radio modified with a probe wire around the IF can to cheaply and reliably "sweep" a room for video surveillance. Of course, many video cameras are fake look-alike devices installed for security purposes. The AM radio device can be used to verify whether a camera is real and operating or just a dummy camera.

Take the sensor device around a room and notice the various noises it makes when placed near TV sets, fluorescent lights, computers, calculators, and some digital clocks and watches. Just about anything electronic will produce an identifiable noise "signature" with this device.

This is another example of low-tech off-the-shelf hardware being used to solve a high-tech problem. There are numerous devices that can be employed creatively to solve technical problems you may encounter. Use your imagination and improvise.

Improvised Hook Switch Alarm

Although it is possible to simply monitor the VOM reading at the hookup terminals of a bypassed line in order to learn if the subscriber is attempting to use the seized line, many times the seizure is done at night some distance from the target building. In this situation there must be a means of alerting the operative that the user has attempted to make a call and is now aware that the line is not functioning.



This homemade hook switch alarm provides audible and visual warning when a seized/bypassed telephone line is picked up.

The circuit in the illustration on page 206 is simple and inexpensive to build. It requires only three components and a 9-volt battery. It can be built on some *perforated phenolic board* (or *perfboard*) or on a thick piece of cardboard or plastic. The device fits inside a pack of cigarettes with ease.

The following parts are required for construction:

1. PC MOUNT 5K OHM POTENTIOMETER (Radio Shack stock #271-217).
2. 3.6 Khz 4-28 VDC PIEZOBUZZER (Radio Shack stock #273-060).
3. 7.2 VDC PR-18 FLASHLIGHT BULB (Radio Shack stock #272-1168).
4. 9 VDC RADIO BATTERY.
5. BATTERY CLIP (Radio Shack stock #270-325).
6. HOOKUP WIRE.
7. MINI ALLIGATOR CLIPS (Radio Shack stock #278-1156).
8. SOLDER, ETC.

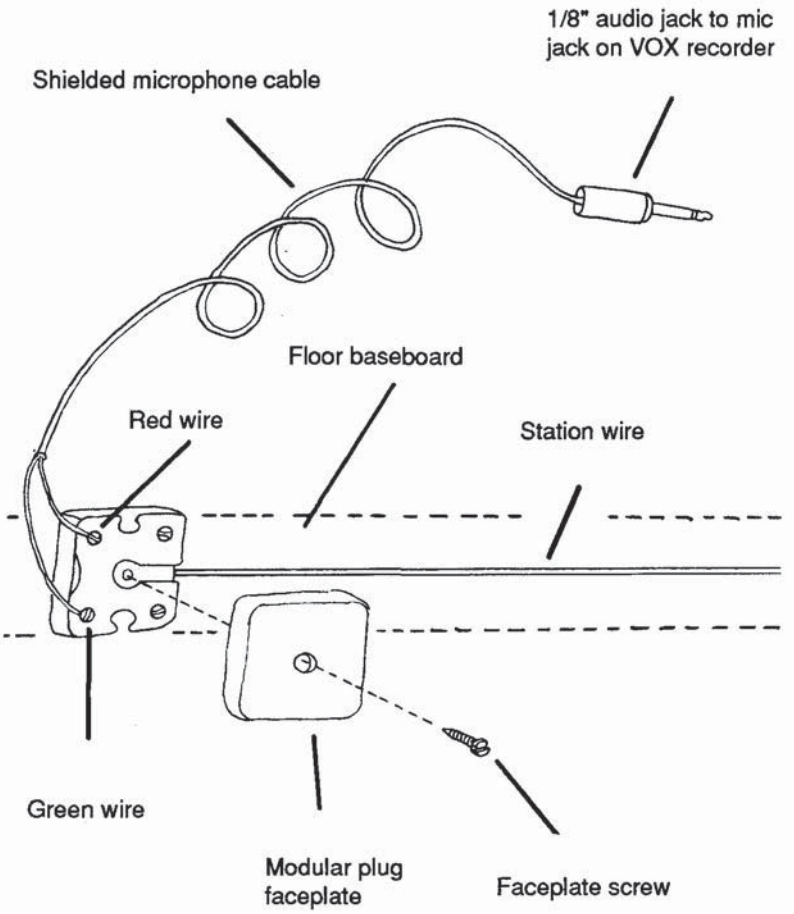
As you can see by the illustration and schematic, this device is not complex or difficult to wire. To use, simply bypass the target line and adjust the potentiometer so that the light energizes and the buzzer sounds, then bring it back down until the light goes out and the buzzer stops. If the line is picked up, both light and buzzer will energize.

Phone Tapping for Account Code Collection

There are two types of hardware employed in telephone wiretapping: direct and inductive devices. An inductive collection device is simply a small coil of several thousand turns of fine-gauge wire placed near the phone line. When the phone is being used, the electrical signal is detected and transferred to a tape recorder without having to connect anything directly to the line.

There are several points on a typical pay telephone where an inductive collection device can be attached to provide the required traffic. A low-cost inductive phone

pickup coil is available at Radio Shack (stock #44-533) for a couple of dollars. This device plugs into the microphone jack of a cassette recorder and provides excellent pickup. Tapping a busy pay telephone at an airport or bus station with an inductive device can result in the mass acquisition of telephone credit card numbers.



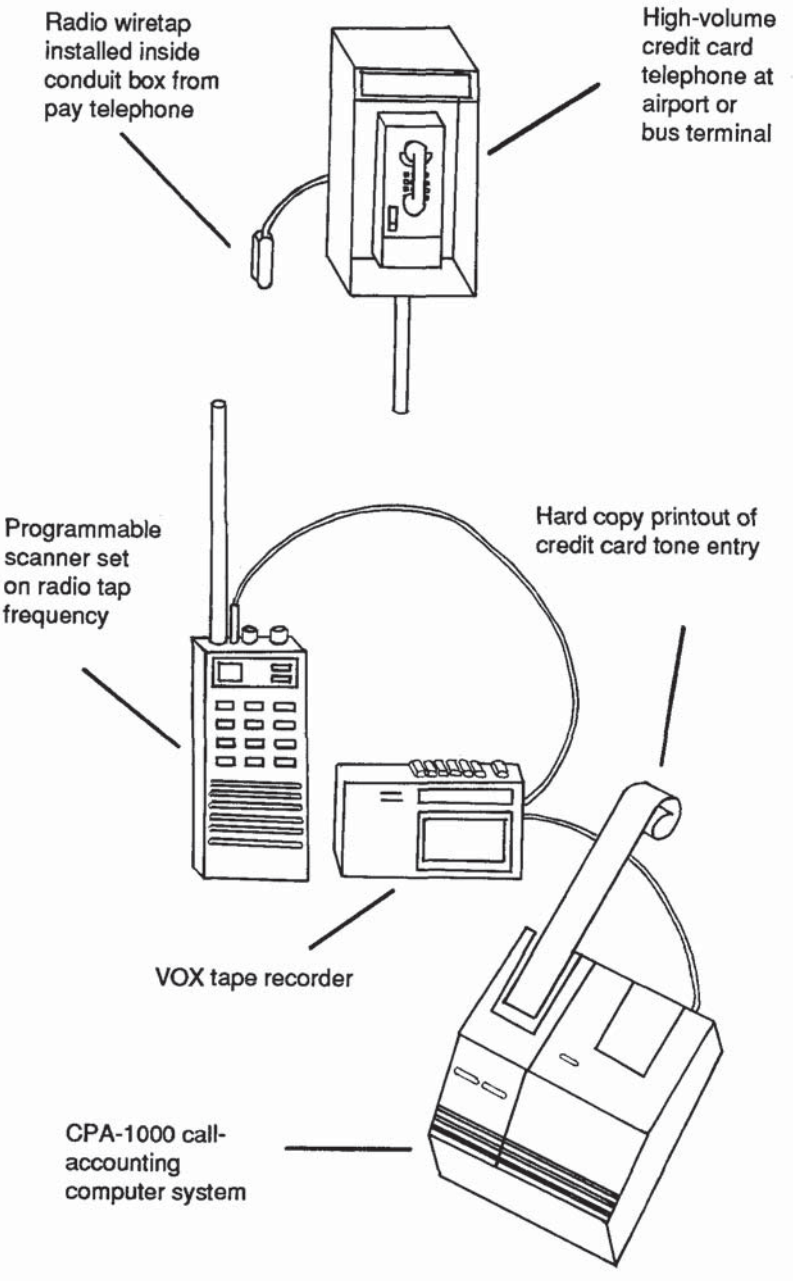
A fast and simple low-cost wiretap. The shielded microphone cable can be plugged directly into a VOX recorder.

Newer cassette and microcassette recorders have a feature known as *VOX*, or *voice activation*, that is useful for wiretapping applications. By simply connecting the phone line directly into the microphone jack, the recorder will only turn on and record when the phone is in use. For example, many pay telephones utilize standard grey D station wire, making them excellent target phones. Using flame splicing or insulation displacement, a recorder can be connected to the red and green wires inside the station wire. The illustration on page 208 shows another application of this simple, low-cost phone tap.

A parasitic telephone wireless transmitter also can be hooked up to the red and green wires to transmit the telephone traffic to a receiver and recorder. The DECO Industries model WTT-20 is quick to assemble and inexpensive, yet it will broadcast both sides of a phone conversation several blocks without batteries, since the device uses the phone line's electricity to function.

Regardless of how you collect the phone traffic—inductively, directly, or by radio—if you make a good quality recording of the conversations and tone dialing, any numbers not given verbally to the long-distance operator can be collected from the tape with a low-cost decoder. A call-accounting device such as the Radio Shack CPA-1000 (stock #43-152) can be connected directly to the target phone line to provide an accurate digital printout of all phone numbers dialed on the line. Recorded traffic can also be played directly into this device with a home-built modular adapter from the recorder's earphone jack. The CPA-1000 runs off four AA batteries, which allows operation without having to plug it into a wall socket.

As you can see in the illustration, a radio wiretap can be inserted inside the conduit box that typically houses the station wire in back of the pay phone. WARNING: Many pay telephone terminals have two such conduit runs in back. One of these contains a 110-volt AC wire


Radio wiretap installed inside conduit box from pay telephone
High-volume credit card telephone at airport or bus terminal
Programmable scanner set on radio tap frequency
Hard copy printout of credit card tone entry
VOX tape recorder
CPA-1000 call-accounting computer system

that provides the booth with electricity for lighting, etc. Carefully open the conduit housing with a screwdriver and observe the thickness of the wire. If it is heavy gauge and multicolored—such as black and white or green—then this is probably the power cable. The conduit containing the telephone station or drop wire will be light gauge, solid strand. Handle these wires with caution until you have identified them. You can receive a substantial shock from the wiring.

It is frequently desirable to hook up a small piece of wire to the radio wiretap to serve as an antenna. If the tap is concealed inside the metal housing of the conduit, a small piece of wire should be left dangling neatly outside the housing to allow efficient radiation of the signal.

The radio tap is received by a scanner, which then feeds the signal to a VOX recorder. The recorder's output is fed into the call-accounting computer, which provides the operative with a detailed printout of all credit card numbers or phone numbers dialed into the target telephone. The call-accounting system can also provide data on the time calls were made, the duration of each call, hang-up time, and the number of rings before connection was made. All this can be useful information.

All of the above devices will run on batteries, and the entire system can fit easily into a typical attaché case for portable collection work. If several devices are installed, the scanning receiver can continuously scan a number of pay phone wiretap frequencies and begin recording only when one is in use. Long-distance credit card calls from a pay telephone tend to be quite short, and if an extended play

A wireless, unattended radio wiretap. This low-cost (under $300) system can provide both sides of telephone traffic as well as a continuous printout of all long-distance credit card numbers dialed. It can be assembled to fit inside an attaché case and allows interception of up to 100 telephones in a prearranged priority.

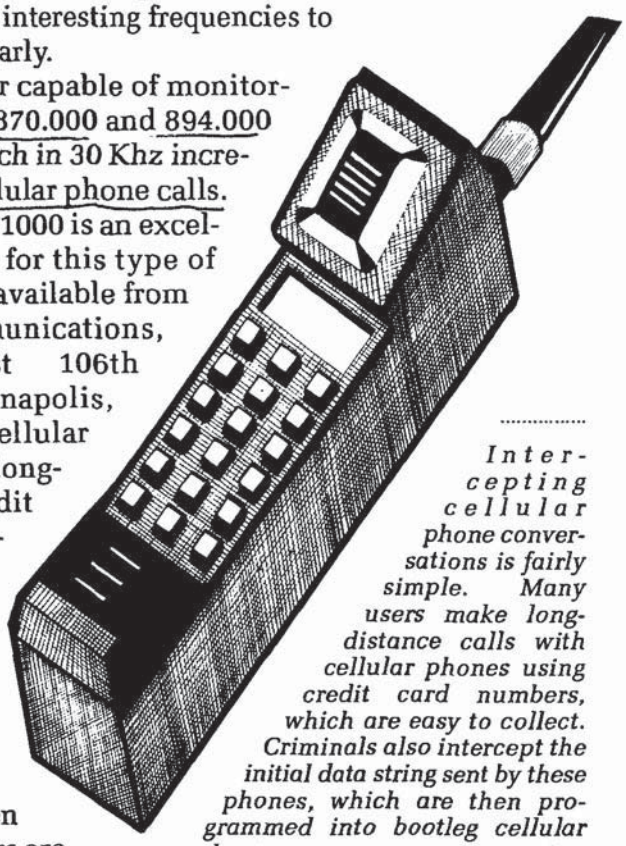
recorder is used, one two-hour tape can provide the operative with dozens of working telephone credit card numbers in less than one day from a busy transportation center.

Collecting Telephone Credit Card Codes with a Scanner

A programmable scanner capable of monitoring between 46.000 and 46.980 Mhz can easily search all the frequencies available for cordless phones (as well as the new allocations issued by the FCC coming on line in a couple years). Many people who use a friend's cordless phone to make a long-distance call will use their credit card, giving the number to the operator over the airwaves. Thus these are also interesting frequencies to monitor regularly.

A scanner capable of monitoring between 870.000 and 894.000 Mhz can search in 30 Khz increments for cellular phone calls. The ACE AR-1000 is an excellent scanner for this type of monitoring (available from ACE Communications, 10707 East 106th Street, Indianapolis, IN 46526). Cellular owners use long-distance credit cards frequently, and they, too, often read the numbers to the operator over the air.

Even when these numbers are



Intercepting cellular phone conversations is fairly simple. Many users make long-distance calls with cellular phones using credit card numbers, which are easy to collect. Criminals also intercept the initial data string sent by these phones, which are then programmed into bootleg cellular phones.

keyed into the cordless or cellular phone manually by the user, a digital DTMF (dual-tone multifrequency) decoder available from a number of electronics suppliers will provide you with the numbers.

2) ACCESS CODE INTERCEPT

Access to or possession of long-distance telephone credit card codes is a useful underground communications tool. The codes allow an operative to go to virtually any one of 570 million telephones in the world and place a call to any other telephone.

The organized theft of telephone long-distance credit card access codes has been conducted for a number of years. This activity is perhaps the most financially draining service theft for the various long-distance carriers. Where a simple approach to service theft such as parasitic interconnect is focused on the operative's private use of the phone circuit, *access code intercept* provides criminal groups with a source of income. The account codes are sold nationwide through computer bulletin boards, underground criminal networks, and at major transportation centers.

The previous section on parasitic interconnect provided details on using a radio wiretap for the mass collection of usable access codes from pay telephone terminals as well as how to acquire these numbers with a programmable scanner. This section will focus on nonelectronic collection of these codes.

Since this is such a problem for the telephone companies, the illegal acquisition of access codes is aggressively studied and prosecuted within the industry. This activity is potentially the most dangerous of all approaches for an underground operation. The legal ramifications of being taken into custody for possession of a stolen account code number or collection of account codes should not be understated. The process

by which the average service thief is eventually caught is important to consider.

If you use a stolen credit card number to call anywhere but another pay phone, you will eventually be detected and caught. Toll analysis for patterns of theft has become highly advanced.

The chronology of the illegal calls is of major importance to establishing a pattern. The first call or two is often used by the specific thief; it may also be used to disseminate the code number to others. Thus if the first illegal call originates in one area code and is used to call another area code, and if subsequent calls originate from the second area code thereafter, the security analyst will know the card was probably stolen in area code one and then sold in area code two. The fact that the chronology of the calling pattern is significant should convince the reader that allowing a large number of people to use the number after you have used it for a while will do nothing but accelerate the detection process.

There are four basic nonelectronic access code collection strategies currently being employed:

1. NONINVASIVE POSTAL INTERCEPT.
2. TELEPHONE SOLICITATION FRAUD.
3. RETAIL SALES TRANSACTION IDENTIFICATION FRAUD.
4. TERMINAL SURVEILLANCE.

An understanding of these methods of credit card theft and fraud will provide the operative with several options in the use of the telephone.

WARNING: The following techniques are illegal. It is a criminal act to conspire to defraud the consumer or the telephone company to gather information regarding long-distance telephone credit card numbers for the purpose of illegal usage. There are federal penalties for conviction of such crimes.

This is an important consideration in communications planning. The theft of access codes for free long-dis-

tance calls is a somewhat useful capability, but it is not the safest communications tactic in the world.

The methods used by small-time service thieves are easy to understand and relatively simple to employ. A professional thief, on the other hand, will never personally use the code number. It is a perishable "commodity," used as a currency in street crime. Selling the numbers in groups of five for $100 is common. The distributors of the stolen numbers are not greatly concerned with the toll billing analysis threat, since no traffic on the bill will ever be linked to them. This operational characteristic is what makes telephone access code intercept a lucrative multimillion dollar industry.

The communications officer frequently has a different use for the numbers than the typical service thief. Overall, however, bulk intercept of access codes by electronic and nonelectronic means is probably not a very effective or useful tactic in any long-term guerrilla underground enterprise. This technology is only useful in short-term or emergency operations. Careful use of COMSEC is advised. The communications officer must control the distribution of both the numbers and the collection technologies, since all aspects of the process are illegal and potentially compromising.

The network that would employ the stolen access codes on an ongoing basis is the action net. These cell members tend to be mobile to the degree that they can be considered transients. The random use of an illegal card to contact another mobile member of these frequently fragmented cells is practical and common.

Noninvasive Postal Intercept

This is a relatively new approach to credit card theft. The service thief has learned that if the telephone credit card is mailed to a customer and it is not received because of postal intercept, the card will be cancelled immediately. This is a direct result of BELCORE's mail

accounting program. Consequently, the thief now uses a few creative techniques to gain access to the number without opening the mail or even needing to have possession of the mail for a significant period of time.

The telephone credit card is usually mailed in a distinctive envelope that carries the long-distance company's logo on the outside. The envelope also has a characteristic thickness. Service thieves specialize in identifying these packages.

By feeling the envelope and bending the package slightly, a service thief can determine that it does in fact contain a plastic card. The thief simply places a piece of thin paper over that portion of the envelope and carefully rubs over it with the side of a sharp pencil to create a stencil image of the embossed numbers.

Another approach used by college students is to place an ordinary piece of typing paper over the card location and then put a piece of carbon paper over that. They then run a plastic card or a comb over the carbon paper and it imprints the card number from the carbon to the typing paper.

If the card is not embossed, then the service thief sprays the outside of the envelope with a small amount of automotive Freon normally used to recharge automobile air-conditioning systems. The Freon makes the envelope transparent or at least semitransparent. The card number is read and transcribed before the Freon evaporates without any visual trace on the envelope.

"Wet" openings using high concentrations of steam are less effective on these types of mail packages because the seal on the envelope is gummed and closed by a machine; therefore the sealing compound is seldom water-soluble. Since the package is produced by automated means, the old style "dry" openings also tend to be ineffective, since the piece is tightly sealed.

Postal intercept of credit card account codes has many risks and is seldom practical unless the operative has access to a high-traffic, high-turnover residential area. For

instance, college students returning to campus generate a large number of telephone installations in dormitories in a relatively short period of time. This high volume of service connections and long-distance access card mailings has significant appeal to the service thief. Military housing facilities also tend to have a high turnover and, subsequently, a lot of new service connections.

Mail intercept of card numbers is especially dangerous since phone service theft is only secondary to the serious crime of tampering with the U.S. Postal Service. The mail is the property and legal jurisdiction of the federal government until it reaches the intended recipient. Tampering with the U.S. mail is a federal offense.

A recent case of a phone company sting operation should be considered by the operative.

In 1989, a major U.S. long-distance carrier mailed a large number of false telephone credit cards to a college campus. If the card was actually received by the intended user, the carrier offered the service on a trial basis so he or she could compare the carrier with their current long-distance service. The parties who intercepted any of the temporarily active account codes were caught because every bit of traffic on the card numbers was recorded and traced by the carrier.

Telephone Solicitation Fraud

Telephone solicitation fraud is notable because it is somewhat anonymous and it gains access codes by simply asking for them. It, too, is a relatively new approach to gaining access to telephone credit card numbers.

The long-distance service industry is extremely competitive. An increase of a fraction of one percentage point in market share for a company can mean literally hundreds of millions of dollars in increased revenues. As a result of this lucrative business climate, many firms conduct aggressive telemarketing campaigns to sign up new customers. Exploitation of this

situation by criminal groups has proven extremely difficult to defeat.

A telephone "solicitor" will call random residential numbers out of the phone book. He will tell the person who answers that he represents one of the major long-distance carriers or a "new" fictitious carrier. The solicitor frequently targets a specific demographic group in this enterprise. For example, he will offer elderly prospects a substantial "senior citizen discount" for giving the fictitious company a trial run. He will then offer one or more free months of service to the prospect if they agree to a trial. The deal offered is never too good to be true, but the savings are usually quite substantial to the senior citizen.

The solicitor gets the prospect to agree to a no-obligation trial period with one free month of service. Once the agreement is made, the solicitor asks the person for his current long-distance carrier account number so he can notify that company that the person wants to switch over for a trial period. The solicitor tells the person that he does not need to contact his current company himself unless he decides to keep the new service. As soon as the prospect gives the solicitor his long-distance credit card number, he is told that he will receive confirmation and brochures in the mail in a couple weeks.

Of course, the prospect never hears from the solicitor or the bogus company again, and his credit card number is used by various criminal groups until it "burns," or no longer allows long-distance access.

The smooth-talking phone solicitor can gain a large number of telephone credit cards this way in a three or four hour shift. Elderly and low-income housing occupants seem to be the most frequent targets, although recent telephone solicitation fraud operations have focused on college campuses.

The various carriers have studied this problem, and the fact that most of them participate in their own long-distance service telemarketing programs seems to keep it

from being corrected. Most American households receive these solicitations from time to time, and there is no practical way for the prospect to identify the solicitor or the validity of the offer being made.

TELCO Security Ploy

This is a fairly sophisticated variation of telephone solicitation fraud that allows the operative to get a quick set of numbers for emergency use. The operative seizes a line and determines which long-distance service his target is using by making random calls or by using the 700 code. Basically, the line is seized from outside the residence (apartment complexes are frequent victims of this approach because the terminal and junction boxes generally are accessible to the operative) and the thief dials 1-700-555-4141. This accesses the long-distance switch, and a recorded voice identifies which carrier is using the line.

The operative then calls the target from a pay phone and in an authoritative voice identifies himself as an employee of the security division of that long-distance carrier. He tells the target that he is checking the toll billing of the target's long-distance account to determine if it has been tampered with. He reads a series of numbers to the target and asks him or her, "Are any of these your long-distance access code?" The target states that none of them are. The "security man" then asks for the correct number, and amazingly, the target often provides it. The target is then advised that there was probably some sort of mix-up and that he will not be billed or contacted again regarding the problem.

This ploy has many variations and is frequently targeted toward elderly people. Once the operative gets the legitimate credit card number, he reassures the target that he will "straighten things out" and apologizes for disturbing him or her. The operative often has a legitimate number of the carrier should the target ask for it, but this number is for an obscure billing inquiry office or other toll call

center in another state. The target is often hesitant to pay for the long-distance call to inquire further but feels reassured that there is a number to call should they have any questions.

The numbers are burned very rapidly. Generally, within a matter of days, the customer's card has hundreds and even thousands of dollars of unauthorized usage by the time the real phone company security calls to inquire about the irregularly high usage. By then, of course, it is too late. The card is cancelled and the customer is issued another. Although they are warned about the ruse, they typically do not have to pay the unauthorized charges.

Retail Sales Transaction Identification Fraud

This approach was recently uncovered in New York City. A group of retail clerks were already involved with selling major bank credit card numbers to a criminal group. They began making a sideline out of obtaining and then selling long-distance access codes to the same source. Every time a customer wished to pay by check, the clerks accepted a bank credit card as ID for the transaction, but the customer was then requested to present another form of "plastic" and they were told that a telephone card was suitable.

Consumers are hesitant to provide their bank credit card numbers in order to cash a check, but they seem to be more than willing to provide their telephone credit card number as a piece of identification. The fact is that a telephone credit card is not a usable form of ID, and theft of service from a phone credit card is easier to accomplish than theft off of a bank card.

Many people do not have major bank credit cards, but if they have a phone they generally have at least one long-distance credit card. This approach is difficult to defeat, although if the customer remembers using the card to cash a check, the clerk is very likely to be questioned by a telephone company investigator.

Another ID fraud scheme involving false solicitation for a major bank card was uncovered recently in a low-income housing project in Chicago. The solicitor offered a guaranteed bank credit card to someone in a low-income situation and asked for his telephone credit card number as part of the application. This criminal technique is also relatively difficult to counter.

Terminal Surveillance

This is one of the oldest techniques of telephone credit card account number theft. Basically, it is the technique of observing someone dialing in a credit card number at a pay phone terminal in an airport or hotel lobby.

Terminal surveillance is actually a variation on an age-old technique taught to surveillance operatives at many law enforcement and intelligence agencies. The ability to follow someone on foot and observe them at a pay telephone while making careful note of the numbers the subject dials can be very useful.

Entire rings of credit card thieves have operated using this technique as their sole source of code number collection. The thief, sometimes called a *watcher*, situates himself near a large bank of pay phone terminals in an airport lobby. He has a usable cover reason for sitting there, such as waiting on a traveler. The successful watcher works any one location only for a short period of time before moving around on a predesignated route in the air terminal.

Although most airport security personnel are knowledgeable of the theft of passenger telephone codes through terminal surveillance, it is relatively difficult to detect someone in the act of number collection. There are a number of much more serious crimes that occur at air terminals, so this activity is not heavily focused on by security personnel.

In the mid-1980s, terminal surveillance activities were covered heavily in the press. Many newspapers and magazines advised travelers to dial their credit card num-

bers in a manner that would be difficult to observe. Despite the warnings, the typical traveler either is not aware of this threat or is not concerned by it. By visiting a local bus or air terminal during passenger boarding and arrival, you will see that there are more numbers being visibly dialed into more telephones than you can easily make note of. (A group in Los Angeles even provided its watchers with microcassette recorders to read off the numbers observed being dialed into phones.) These conversations and phone contacts tend to be fairly brief; thus, more numbers are used per phone, per hour.

The thief tends to target a specific passenger profile to surveil at a phone bank. The well-dressed business executive may use a company phone credit card to make his call, and the corporate card is a prized number to acquire. This particular type of access code number is termed a *double zero* in street slang because many companies have the last four numbers of their office telephones in the hundred and thousand series, such as 555-2300 or 555-2100. These are already high-traffic codes, and the various employees who use the card daily frequently use it to make personal calls as well. This places a considerable volume on these cards. If used sparingly by the service thief, the access number will be good for several months. If he uses it only to call "sterile" numbers, the theft may never be detected.

Using a high-volume card immediately after the legitimate holder of the card used it also helps conceal the theft to a degree. The user of the card will get the bill for your usage but may not remember what specific calls were made that day, or to where. The user will, however, remember being at that location and making a call.

A trained observer at a telephone bank can develop the instinctive ability to detect other surveillance in the immediate area. After sitting at a high-traffic phone bank for any period of time, the operative can easily point out anyone else conducting the same type of

surveillance as well as any security personnel observing the entire area.

Testimony that an individual was observed sitting near a phone booth apparently watching people dial in their card codes is not considered permissable evidence in court. A subject must be caught transcribing the number to some medium. Many thieves write the numbers they collect in a magazine or newspaper they appear to be reading while conducting the surveillance. The group using recorders in Los Angeles avoided prosecution for some time because they trained all of their watchers to record a maximum of five numbers and then rewind the tape back to the beginning. If the watcher detected surveillance, he was instructed to leave the area immediately. If he was challenged, he pressed the record button to erase the five numbers in seconds while politely stalling the individual challenging him.

Terminal surveillance is simple, successful, and incredibly common throughout the world. The ability to quickly employ the technique to collect just one usable telephone credit card number to make just one quick telephone call is a significantly useful form of tradecraft. A skilled operative should always be able to go to any airport and immediately collect an account code or two, then go to any pay phone in the area and make a contact.

The conduct of this simple operation can also provide an added layer of COMSEC for an underground operation because it can be used to spontaneously create a significant amount of electronic "litter" should the operative happen to be at an airport and suddenly detect active surveillance. The people watching the operative probably will not observe one quick code collection, but they certainly will observe the use of a telephone afterward. They may even make note of the numbers dialed. A time-consuming deceptive "lead" can be created if a random number out of the local directory is called. The investigator will have to follow up on whatever number was

called, and he will also have to check out the owner of the credit card number used. When the investigator confronts the owner of the credit card, he will deny knowledge of knowing the operative, even though he *was* at the airport on that specific day at that specific time. This is a potentially time-intensive false lead to give to any government or private intelligence agency.

SYSTEMATIC DECEPTION

Systematic deception is a relatively simple yet difficult-to-defeat technique that requires a small amount of planning but ultimately results in the operative obtaining at least three long-distance access codes by making just one fifteen-minute phone call. It entails simply asking the phone company for access under a fictitious name. This technique takes advantage of an operational characteristic of the telephone long-distance service industry and is employed by undercover operatives, corporate intelligence types, and criminal conspirators.

When the telephone billing office receives a request for residential telephone service, the entire order is processed over the phone. If the customer's residence has had service recently or has modular jacks already installed, the activation of the line requires central office control only, meaning no technician has to visit the residence to connect the service. It is a relatively simple task to locate a suitable unoccupied dwelling to establish as a fictitious residence for a service installation request.

The verbal application over the phone establishes an immediate credit "profile" that the operator can use to instantly grant a connection on a specific day and time. Since the connection will be made at the central office, the customer does not need to be home at the time service is connected. The operator simply provides the new customer with an installation date and the new telephone number, usually right at the time the

service request is made. Connection generally takes a few working days to complete.

Systematic deception exploits this lack of human interaction for a typical telephone service connection. Using this technique, the operative creates a false "electronic identity" and obtains an unlisted telephone number in a fictitious name in an unoccupied dwelling. Using this newly assigned telephone number and false account, he contacts the various long-distance service carriers in his area and obtains telephone long-distance travel cards or actual long-distance service. The phone line installed at the false residence is never actually used by the operative; it and its accompanying billing account are used only as a basis to get account cards from long-distance carriers.

This anonymous approach to long-distance service access has many significant advantages over outright service theft. Eventually, the initial service will be disconnected for lack of payment, usually within sixty days of connection. However, the long-distance cards can last for over a year if they are not used heavily. Eventually these too will be cancelled for nonpayment, and the closed account becomes nothing more than uncollectible accounts receivable to the phone companies rather than an apparent theft of service. The account is not studied by security investigators; instead it is placed with the collections department for follow-up to try and recover the unpaid bill. Eventually, the entire account is written off as "bad debt" and the effort to collect is suspended. The entire matter goes into the "dead" file, and the file is kept only to deny service to the fictitious name if it is ever requested again.

Creating an Electronic Identity

Systematic deception requires an electronic identity that will meet specific credit profiles for the telephone company's business office. When you call to request phone service, the operator will ask a few questions to

determine your credit worthiness as well as verify your identity. The following information needs to be provided:

1. FULL NAME.
2. DATE OF BIRTH.
3. SOCIAL SECURITY NUMBER.
4. PREVIOUS ADDRESS AND PHONE NUMBER.
5. CURRENT EMPLOYER.
6. BANK REFERENCE.
7. CONSUMER CREDIT INFORMATION.
8. TWO OR THREE LOCAL NUMBERS OF FRIENDS, FAMILY, OR ASSOCIATES.
9. ADDRESS FOR PHONE INSTALLATION.
10. TELEPHONE SERVICE OPTIONS.
11. BILLING OPTIONS.
12. PREFERRED LONG-DISTANCE CARRIER.

Unlike other forms of false ID, an electronic identity is relatively easy to create since there is no actual documentation involved in its creation. The following pages will discuss methods of creating this unique form of identification that will enter the telephone company's computer without a hitch.

Carefully applying the following steps to create your false electronic identity, destroying your notes when finished, and destroying the credit cards you gain using this technique will significantly reduce the chance of compromise.

WARNING: Providing a fictitious name to a business with the intent to commit consumer fraud is a felony in all states. Providing a fictitious Social Security number to any business or agency is also a felony. Possession of a long-distance telephone credit card that was obtained using false pretenses is sufficient grounds for prosecution. Conviction of conspiracy to defraud may result in a $100,000 fine and/or ten years imprisonment.

STEP ONE: *Create a name.*

To assist in the approval of your phone service, create a common name for yourself. The more common the name, the more difficult to track potential abuse. Ac-

cording to the U.S. Census Bureau, the following are the ten most common names in the United States:

1. SMITH.
2. JOHNSON.
3. WILLIAMS.
4. JONES.
5. BROWN.
6. MILLER.
7. DAVIS.
8. ANDERSON.
9. WILSON.
10. THOMPSON.

Your choice of first and middle names is flexible. Although you generally are asked only for a middle initial, it is best to have a complete middle name handy in case one is requested.

STEP TWO: *Create a date of birth.*

This may sound simple enough, but there are some parameters that merit consideration. First of all, don't use your real date of birth; it could be used as a means to catch you. Second and less obvious is your age. Make your age at least 35 years old. People in the 35 and older group are much better credit risks than those in younger age groups. Compute your current age based on your fictitious date of birth and put it on the notations beside your date of birth. Don't get tripped up by knowing your date of birth but not your age.

STEP THREE: *Create a Social Security number.*

Your Social Security number is the most useful identification for a business or the government to maintain various records on you. Again, it obviously is not a good idea to provide your own Social Security number. As a matter of fact, it is wise to avoid even slight resemblance to your own number.

In this operation you are going to be someone who just moved to the area, and where you moved *from* has some bearing on the Social Security number you choose. The

NEW JERSEY 135-158
NEW MEXICO 525
NEW YORK 050-134
NORTH CAROLINA 237-246
NORTH DAKOTA 501-502
OHIO 268-302
OKLAHOMA 440-448
OREGON 540-544
PENNSYLVANIA 159-211
RHODE ISLAND 035-039
SOUTH CAROLINA 247-251
SOUTH DAKOTA 503-504
TENNESSEE 408-415
TEXAS 449-467
UTAH 529
VERMONT 008-009
VIRGINIA 223-231
WASHINGTON 531-539
WASHINGTON, D.C. 577-579
WEST VIRGINIA 232-236
WISCONSIN 387-399
WYOMING 520

It is notable that the further south and west on the map, the higher the first three digits of the Social Security number. HINT: Create the Social Security number from a populous state. Note that some states have more numbers available than others; California, for instance, has twenty-eight three-digit codes, while Alaska only has one.

A credit check based on a Social Security number and complete name is fairly expensive. The various agencies that sell this information do so at a cost of about $25 to $50 per inquiry. This makes it expensive for the phone company to actually request these reports for each new account. The credit worthiness of the service requester, therefore, is based on the answers given to the questions at the time of the request. No actual credit checks are gen-

erated in this process unless the caller is requesting a number of lines for a business.

Although the Social Security Administration is prohibited by federal law to verify or provide Social Security numbers to any commercial enterprise as well as most federal agencies, the threat of being caught with using a false number should be considered carefully. It is a felony to use a bogus number on a job application as well as when applying for a credit card or consumer credit, and a bogus number would not pass a law enforcement or detailed credit inquiry, such as one made during an arrest or during the purchase of a large-ticket item. Since the operative is not actually filling out any documents when requesting phone service, the criminal risk is lower, but it still should be considered.

STEP FOUR: *Create a previous address and phone number.*

The further away from the place you request service the better. If you are getting a bogus installation in Florida, make your previous address in California or Oregon. It is preferable to have actually been to the city listed as your previous address. By using one of the common names discussed earlier, it is possible to go to the local library and look up your previous address in one of the many phone books available there. Although you can certainly make up the entire address and phone number, it is best to have an existing one to use. If you use one of the common names given above, you will be surprised at the number of addresses and phone numbers available to you.

One final insurance would be to gather several potential previous numbers and call them collect from a pay phone. Odds are very good that, if chosen from an older phone book, one of these numbers will be disconnected. The disconnected number is the one that you should use along with its accompanying address.

Learning the ZIP Code to your previous address is

also important. Find it in the beginning of the phone book or in the library's ZIP Code directory.

The above method takes advantage of another characteristic of the new phone system. Since the regional phone companies are no longer related to one another, it is difficult for any one company to verify information about you from a different company, particularly if that company is far away from where you are making the bogus request.

STEP FIVE: *Create a current employer.*

Your new identity has just hired on to or been transferred by the biggest company in town. Learn the exact address of this company as well as the phone numbers to the main switchboard and your specific department.

Choosing a large company helps you create legitimacy and financial solvency in the mind of the operator, and a common name is likely to be found in most any department. This information is not usually checked out either, but it is a useful ploy to create legitimacy.

STEP SIX: *Create a bank reference.*

Tell the operator you have a checking and savings account at a local commercial bank or savings and loan. You will be asked for a number to these accounts, and they can be created rather easily.

In the lower left hand corner of a bank draft or check is a series of numbers printed with a magnetic ink, and their use is fairly standardized. Typically there are twenty-five digits, which represents the following information:

Federal Reserve Bank ID number	Individual customer account # account number	Check number
123456789	123456789000	0123

By looking at a check from a local bank, you can create a false account number. Tell the operator you are looking at the bottom of your check for your account number. As long as you get the first nine digits right and provide

eighteen more numbers to the operator, you will have no problem. Banks generally are hesitant to provide credit information to anyone by telephone. This typically eliminates the operator's ability to verify the account.

STEP SEVEN: *Provide consumer credit information.*

Indicate that you have a late-model vehicle you are paying off through a bank loan, as well as several accounts at major department stores. This frequently is a cursory question to determine if you have consumer credit; it is seldom too specific in nature.

STEP EIGHT: *Provide local contact numbers.*

The service operator will ask for the names and telephone numbers of people you know locally. Although this is requested as another form of credit reference or a way to get ahold of you in case there is a question with your installation, it is also to provide the phone company with local sources of information should you fail to pay your bills. These names can be provided to the operator directly out of the phone book.

STEP NINE: *Provide an address for phone service installation.*

This is where you are requesting service. It should be a densely populated, upper middle class apartment complex or housing development. The actual apartment number should be known and provided. When selecting an address, consider access to the mailbox of this dwelling in order to be able to retrieve the account cards when they arrive. Another option is to set up a fictitious mail drop and use it to collect the account cards. It is not uncommon for phone customers to request that bills be mailed to a post office box or an address other than the service location.

STEP TEN: *Choosing service options.*

Frequently the operator is given a bonus for meeting quotas on selling such options as call waiting and call forwarding. There is a degree of flexibility here, but it is suggested that you request an unlisted number. About 40

percent of Americans now have unpublished numbers, paying a small fee each month to keep their names out of phone books and off of directory assistance. This desire for privacy is encouraged by the phone company, since it gets paid to provide the service. It's also a good idea to order some other option to help the service operator fulfill his or her quota and thus encourage the smooth flow of the process.

STEP ELEVEN: *Choosing billing options.*

After installation and option fees are calculated, the usual cost for service connection is around $50 to $100. It is common for the phone company to allow this fee to be paid over the next three months. If this is offered, take advantage of it; it tends to slow down the disconnection of the false line.

STEP TWELVE: *Choosing a long-distance carrier.*

If you answer all of the questions properly, you will be given a telephone number and a date when service will be activated at the residence. At this point the operator will ask you which long-distance service you prefer. Choose AT&T. The operator will provide you with the number to AT&T and activate the billing information with the AT&T operator. You may also request a local phone company calling card at this time. These cards are offered by all the regional companies and are as useful as an account card from a major carrier.

When providing your electronic identity, make sure you have all of your false ID data in front of you, sound casual and kind of busy, and the request will go quickly and smoothly.

Requesting Long-Distance Service

Requesting service from a long-distance carrier generally involves answering the basic questions outlined above, but be prepared to answer a few others. One of the more common is approximately how much long-distance service you expect to use each month. The average tele-

phone bill in the United States is generally less than $50; indicate that your billing will change from month to month but will not often get over $100 to $150. It is important to sound like a good billing customer from the perspective of the long-distance service operator.

When requesting long-distance telephone service, you will be asked by the operator for a contact number to call back. This formality to verify the request for service typically takes place within two to four hours of the request if you call during normal business hours, which is suggested. It is needed because long-distance telephone carriers are aggressive marketing organizations, and sometimes the salespeople get a little over aggressive. The contact number is used to verify the sale; the verifier generally is a supervisor.

The contact number can be a friend's house (not wise, though relatively safe) or a pay phone. For bulk acquisition of cards, where requesting bogus connections and service is an ongoing enterprise, it may be useful to set up a residential phone at a temporary house and use this number as the contact number. This may be elaborate, but it is a viable option when you consider the number of account codes you can generate with this procedure.

Another approach to the contact number is to order call forwarding and wait for service to be connected at the unoccupied dwelling. This low-cost option allows you to transfer inbound calls to any number you wish. Telling the long-distance company to contact you at the new number makes the service request appear even more legitimate, and you can forward the calls from the dwelling by connecting a telephone setup to the terminal box outside the residence.

Most long-distance telephone companies now offer multiple accounts on each phone, meaning that you can get two or possibly three credit cards by indicating that you want one card for your spouse, one for your children, and one to

use for business only. This is easy to request, and the carriers seem to like to provide these extra account numbers.

Keep in mind while making requests for long-distance service and calling cards that these companies are very aggressive in their marketing, and the multibillion dollar long-distance industry is very lucrative. This causes most of them to be very friendly in their marketing efforts. Indeed, systematic deception works because the long-distance companies are aggressive and greedy, and because most people do, in fact, pay their phone bills.

Remember, when requesting residential telephone service, always ask for AT&T to be your long-distance carrier. The various telephone companies all used to be part of AT&T, and this seems to be good "form" in the service request. It might be helpful to record the conversation with the telephone service office in order to study the process for the next step.

Within about a week, you will receive a local calling card and an AT&T calling card. As soon as you receive them, call MCI, U.S. Sprint, and any other carrier, request to switch over your long-distance service at your fictitious phone number, and get calling cards from each. This will not cause any of the other cards to be canceled until they go unpaid. Don't overlook the smaller firms offering long-distance service. One residential telephone connection should yield at least a half-dozen usable telephone account codes.

Study the envelopes and packages that the cards arrive in. Practice noninvasive postal intercepts to sharpen your ability to gain access to card numbers at will. Train certain members of the cell to recognize the familiar envelopes and task them with obtaining a few numbers.

Within a thirty- to sixty-day period, the local telephone service will be disconnected. Amazingly, the local service calling card tends to work for about a month afterward, and the AT&T, MCI, and Sprint cards are not dependent on the actual service connection for contin-

ued activity. They will burn in a few months on their own due to nonpayment.

By spending a few hours a week selecting and connecting bogus residential phone service, your group can maintain a large number of active, legitimate credit card account codes for long-distance use. Once you establish a "flow" of these cards using this procedure, you will always have a means of contacting any phone in the world.

Systematic deception exploits the nonparticipatory nature of phone service connection as well as the competition between the various carriers. It is simple, difficult to detect, and virtually impossible to defeat. This approach to account code access is unquestionably the most secure and reliable.

A couple of warnings are in order here. You do not want to overdo this tactic. You still want to maintain good communications discipline; in fact, you may consider actually paying for the service that you get connected. Always make certain that you destroy the actual cards you receive; simply transcribe the code numbers and access instructions to a separate sheet of paper, encoding them if possible. Also, always use the carrier's toll-free 800 number to set up service, and *never* call anyone who can be even remotely associated with you. When the phone bill comes in to the mail drop, either pay it or destroy it.

Which brings us to a final warning to the reader, and perhaps a useful intelligence collection technique. Undercover agents who circulate in the strange underground economy in the United States and abroad have developed a unique approach to creating a working file on an individual or interest. Investigative agencies have an inventory of telephone credit cards they use to study the communications of an individual. An operative from an agency will approach a low-level drug dealer, for example, and give him a "stolen" telephone credit card as a means of contacting his connections and associates. The operative

tells the target he can use the card number until it burns. Of course, the operative can then learn where a certain individual or group is getting its product, where a mercenary is getting weapons, and so on by simply monitoring the toll billing records of the card number.

The above investigative technique should turn a few wheels in the reader's head. Regardless of what side you happen to be working, this is a realistic area for compromise. You not only need to control the acquisition of these cards and the distribution of the numbers to cell members, but you must also consider carefully the source of these numbers. Credit card numbers for long-distance access can provide your organization with a reliable international communications network. They also make every contact a potential threat and can destroy your unit.

It is the communications officer's responsibility to protect the communications plan from penetration. He must control access to these cards, advise cell members to use them only in the COMMO plan, forbid them to give the numbers to anyone, and forbid personal calls with them. Also, he should never tell anyone in the organization that the calls are free.

• • • • •

Systematic deception is the most sophisticated approach to anonymous access to the long-distance telephone networks. The risk to the operation still is focused on the content of the conversation, and all COMSEC procedures apply. Use this technique with discretion in your underground enterprise.

Telephone Company Internal Codes

There are a number of useful codes employed by telephone service technicians at the terminal and junction box. These codes are entered into a touch-tone keypad and can provide a great deal of basic information and

access for the covert operator. There are codes internal to each calling area and others that seem to be standardized nationwide. The 700 number used to reveal the long-distance carrier on a line and the #200 code to identify the number of the phone being used are two examples of useful codes that can have a number of advantages in "working" the phone system covertly.

There is one problem in relating various codes, CNA (customer name and address) numbers, and so on in a book such as this: they will be changed by the phone companies in the central office's system-control software. There are a number of publications that regularly divulge these service codes, and they actually do somewhat of a disservice to those who wish to operate secretly within the telephone system.

There is another, much more useful way of getting these codes yourself that eliminates the phone company gaining knowledge of the fact that you have this information. The next time you see a telephone technician, strike up a conversation. Phone line technicians and maintenance personnel generally are public oriented and friendly. They are also very well-trained technically. By simply expressing interest in their occupation while observing them at work, you can oftentimes get them to tell you just about anything you need to know. Be friendly and inquisitive, and you can learn quite a bit about how to manipulate the phone system with service codes. A useful technique is to start a conversation with something like, "Is it true that a phone technician can do ____ by just dialing a certain number into the phone?"

In Europe and other areas of the world, codes are much more difficult to obtain because it seems technicians are more wary of the potential for abuse. Also, European telephone technicians are, as a general rule, better trained and paid than American phone techs.

Regardless of where you are operating, it is seldom productive to attempt to bribe information from a phone

service technician. The tech knows better than to sell codes to gain access to internal long-distance circuits, CNA information, etc. However, technicians who were employed by a major carrier and are now employed by a private company may be more amenable to compensation for such information. Pay-phone technicians who work for private companies often can be helpful in providing a number of clever access codes. Nonetheless, proceed with caution, and use common sense in this activity.

Another useful technique for learning telephone operation codes, service procedures, and even local jargon is simply to monitor TELCO radio transmissions with a scanner. Conversations monitored on these frequencies are very enlightening. Oftentimes a newer, less experienced phone technician will call in by radio for instructions on how to service or access a specific line or system.

While conducting certain sensitive ops such as parasitic interconnects and line tapping, monitoring telephone company radio traffic can be as useful as monitoring local police traffic. Should your deeds be observed or detected, the TELCO radio transmissions may serve as an efficient early warning system.

Although some telephone maintenance vehicles have cellular telephones as their radio link, a substantial amount of traffic can still be heard on the following radio frequencies:

35.160 Mhz
43.160 Mhz
151.985 Mhz
158.340 Mhz
451.175 Mhz
451.225 Mhz
451.275 Mhz
451.300 Mhz
451.325 Mhz
451.350 Mhz
451.375 Mhz

451.400 Mhz
451.425 Mhz
451.450 Mhz
451.500 Mhz
451.525 Mhz
451.550 Mhz
451.575 Mhz
451.625 Mhz
451.675 Mhz
462.475 Mhz
462.525 Mhz

OVERVIEW AND WARNING OF THE RISKS AND PENALTIES

The telephone system can be an integral component in any covert COMMO plan. Its versatility and the general availability of access makes it perhaps the most useful medium for covert communications. Telephones integrate well with other mediums, such as radio, facsimile, and data transmissions.

Understanding terminal wiring practices and having the skill and equipment to operate or intercept within the TELCO system is probably one of the most useful capabilities any underground unit can have. The communications officer should focus time and resources on developing strategies to use the commercial circuit as part of the COMMO plan.

Stealing telephone service or intercepting telephone conversations is, however, a risky activity. Individuals and groups have stolen phone service for decades, and they will continue to do so. Yet it is important to understand that these individuals and groups also are caught every day.

The purpose for providing the operative with different approaches to these activities is to assist in the understanding of how an underground group can operate with-

in the electronic environment of the telephone system. The approaches to phone service theft outlined in this book were selected because, for the most part, they are nearly impossible to prevent. Nonetheless, these approaches are not all that difficult to detect should the opposition or TELCO security decide that your organization is intent on stealing service on an organized or systematic level.

In most cases, the advantages of phone service theft for the underground organization are based on anonymity rather than economics. You can employ many of the techniques outlined in this book legally by simply paying for the telephone service that you use. This is important to consider. In fact, the legal use of telephone services is actually one of the most cost-effective means of communications available for the underground operation. The account numbers themselves can be controlled, and the calling patterns of certain agents and operatives can be monitored by studying the bills. If the operative simply pays all toll charges and keeps the accounts current, the prudent use of the telephone is probably the cheapest means of maintaining covert C^3 for an operation on a shoestring budget.

If you are conducting a particularly sensitive operation and you steal telephone service to keep in touch with elements of your group, you may find a very aggressive and diligent army of corporate security and intelligence types scrutinizing your activities. You may find yourself under active surveillance, your calls monitored and recorded, and your operatives methodically compromised and caught.

Also keep in mind that you are not the only one with access to this book. Your opposition will likely read this and similar books regarding communications.

Going underground intentionally to operate covertly is just as intense and paranoia-inducing as going underground to avoid capture or prosecution. Living on the

run is, in fact, like living on the edge of your seat at all times. Your thinking can be affected, your sound judgment reduced, and your activities accelerated out of your control. Underground operations often start with a plan that goes wrong as soon as it is initiated. Stuff happens. Intentionally causing risks by stealing phone service will only add to the dangers already associated with your little "enterprise" and can be the downfall of the entire operation.

Corporations and institutions do not like to be targets of underground operations. Governments certainly frown on attempts to topple them. Communications can be an effective tool and weapon against any target, but understand that the participants must live like fugitives, constantly on the run, regularly having to sacrifice comfort and convenience in order to make the mission succeed. There is no glamour or glory in most underground operations. Stealing phone service or participating in any other activity that is inherently risky will add to the threat of compromise. Plan carefully and proceed with caution.

As the communications planner for an underground operation, you will have the most immediate impact on its success or failure. Simply because making free phone calls can be fairly simple and low risk in nature should not necessarily encourage you to consider this activity as the main thrust of your COMMO plan. This approach is the communications medium of criminals, terrorists, and other underworld types who often play a serious game of cat and mouse with a very aggressive opposition. And they get compromised and caught all the time. The nature of their activity is generally much more serious than the act of ripping off the phone company in the process of conducting their operations. It is important to keep the risk relevant to the rewards of your mission.

Even if you are conducting a minor operation and employ telephone service theft as an integral part of your COMMO plan, you can face stiff criminal penal-

ties. As of May 1991, the maximum sentence for conviction of communications theft or fraud in the United States was fifteen years in prison and a fine of $50,000 for each conviction. This is a federal crime in the United States, and the telecommunications industry has a well-funded investigative apparatus that will assist federal and state law enforcement groups with the identification and apprehension of those individuals intent on fraudulent use of its systems.

● CONCLUSION

This book could easily have been double its size and still not provided every available means of covert communications. Your specific technical needs, of course, could not be predicted completely, so the simplest, cheapest, and fastest means of communications were selected for inclusion. Use imagination and creativity to operate and communicate secretly, and consider the techniques outlined in this manual only as an introduction to the methods available to you.

There is a significant risk in using almost all of the tactics outlined in this book, and most could easily compromise your operation should you decide to accept the risks involved. This decision should not be made lightly.

Regardless of your motives for interest in this technology, it is important to bear in mind that many other people will also study this book in detail. Proceed with the knowledge that there are no secrets here that your opposition cannot gain access to.

Use these techniques at your own risk, and share your intentions and knowledge with no one. Underground communications demand that the conduct and the content be protected diligently.

If your intentions are honorable and your activities focused on empowering the weak or oppressed, it is

hoped that this book has provided you with some insight. On the other hand, should you wish to commit criminal acts or hurt people, there are a lot of clever and diligent folks out there who will catch up with you eventually.

Knowledge is power, but it is not a license to abuse power. Don't get so confident that you believe you are capable of operating covertly at the expense of humanity. Using the techniques outlined in this book for abuse of power may cause things to get quite unpleasant for you and your team. Breaking and/or bending the rules to make things better for your fellow man is looked upon and handled much differently than using the same techniques to create some sociopathic enterprise bent on greed or psychotic hate.

Use these techniques with caution, and don't make any foolish mistakes. Have fun, and for God's sake, don't make a mess.